NASA Procedures and Guidelines

This Document Is Uncontrolled When Printed.
Check the NASA Online Directives Information System (NODIS) Library
to verify that this is the correct version before use.

NPG 2810.1
Effective Date: August 26, 1999
Expiration Date: August 26, 2004
Responsible Office: AO / Chief Information Officer

Security of Information Technology

TABLE OF CONTENTS

Effecive Date: August 26, 1999

PREFACE

P.1 Purpose

This NASA Procedures and Guidelines (NPG) implements the NASA Policy Directive (NPD) 2810, Security of Information Technology. The NPG describes the NASA IT Security Program, providing direction designed to ensure that safeguards for the protection of the integrity, availability, and confidentiality of IT resources (e.g., data, information, applications, and systems) are integrated into and support the missions of NASA.

P.2 Applicability

This NPG document applies to all NASA employees and NASA contracts (as provided by the terms and conditions of the contract), where appropriate in achieving Agency missions, programs, projects, and institutional requirements. Facilities, resources, and personnel under a contract or grant from NASA at a college, university, or research establishment are included in the applicability of this document to the extent prescribed by the contract, grant, or cooperative agreement.

P.3 Authority

a. 40 U.S.C. 1441 et seq., the Computer Security Act of 1987, Public Law (Pub. L) 100-235, as amended.

b. 42 U.S.C. 2451, et seq., the National Aeronautics and Space Act of 1958, as amended.

c. 18 U.S.C. 799, Violation of regulations of National Aeronautics and Space Administration.

d. 5 U.S.C. 552, et seq., the Freedom of Information Act, as implemented by 14 CFR 1206.

e. 5 U.S.C. 552a, the Privacy Act, Pub. L 93-579, as amended.

f. 40 U.S.C. 1401, et seq., Section 808 of Pub. L 104-208,
the Clinger-Cohen Act of 1996 [renaming, in pertinent part, the Information Technology Management Reform Act (ITMRA), Division E of Pub. L 104-106].

g. 50 U.S.C. Appendix 2401-2420, the Export Administration Act of 1979, as amended, as implemented by the Export Administration Regulations, 15 CFR Parts 730-774.

h. 22 U.S.C. 2751, et seq., the Arms Export Control Act, as implemented by the International
Traffic in Arms Regulations, 22 CFR Parts 120-130.

i. 18 U.S.C. 2510, et seq., the Electronic Communications Privacy Act of 1986, as amended.

j. 44 U.S.C. 3501, et seq., Paperwork Reduction Act of 1995, Pub. L. 104-13, as amended.

k. Executive Order No. 12958, Classified National Security Information, April 17, 1995.

l. Executive Order No. 13011, Federal Information Technology, July 16, 1996.

m. OMB Circular No. A-130, Management of Federal Information Resources.

n. National Telecommunications and Information System Security (NTISS) 1, National Policy
on Application of Communications Security to U.S. Civil and Commercial Space Systems,
17 June 1985.

o. NTISS 100, National Policy on Application of Communications Security to Command Destruct Systems, 17 February 1988.

P.4 References

a. NPG 2800.1, Managing Information Technology.

b. NPD 2810.1, Security of Information Technology.

c. NPD 2820.1, NASA Software Policies.

d. NPG 1600.6x, Communications Security Procedures and Guidelines.

e. NPG 1620.x, Security Procedures and Guidelines.

f. NPD 1382.17E, Privacy Act - Internal NASA Direction in Furtherance of NASA Regulations.

g. NPD 9800.1, NASA Office of Inspector General Programs.

P.5 Cancellation

This NPG cancels NASA Automated Information Security Handbook (NHB 2410.9A) dated June 1993.

Lee B. Holcomb
Chief Information Officer

DISTRIBUTION:
NODIS

CHAPTER 1. Introduction to NASA`s Information Technology (IT) Security Program

NASA`s IT Security Program is a set of policies, procedures, and guidance for ensuring the security of the Agency`s IT resources. It encompasses IT security management, planning, implementation, and performance evaluation. The IT Security Program covers all IT resources, including but not limited to computers, networks, telecommunications systems, applications, data, and information.

1.1. Objectives of NASA`s IT Security Program

The overall objective of the IT Security Program is to provide direction designed to ensure that safeguards for the protection of the integrity, availability, and confidentiality of IT (e.g., data, information, applications, and systems) are integrated into and support the missions of NASA. The three components of IT resources that require protection are as follows:

a. Integrity--The ability to ensure that information, the applications processing that information, the information technology systems used to run that information, and the hardware configuration, connectivity, and the status of privilege settings cannot be altered during processing, storage or transmission.

b. Availability--The ability to ensure that data, applications, and systems are accessible when and where needed.

c. Confidentiality--The ability to ensure that information is disclosed only to those who have a valid need to possess it.

1.2. Philosophy of NASA`s IT Security Program

NASA`s philosophy for its IT Security Program is based on the following concepts:

a. Protective controls need to be factored into all decisions concerning IT resources. IT security should never be an afterthought. It must be planned for throughout the life cycle of a system-from project initiation through its disposal.

b. A secure computing environment is based on managing risks to an appropriate level. The security controls applied to a computer system should be commensurate with the magnitude of harm that would result from the loss, misuse, inability to access, unauthorized access to, or modification of the information in the system. A risk-based approach to security promotes using limited resources wisely to protect the most critical systems and information in a cost-effective manner.

c. Everyone is responsible for helping to ensure that IT resources are not exposed to undue risks. Although managers and others in key positions are accountable for preserving the security of IT resources, everyone who uses, manages, or purchases IT resources bears some responsibility for ensuring that integrity, availability, and confidentiality are not compromised.

d. All of NASA`s information is considered valuable and sensitive to some degree. By identifying all of the NASA`s IT resources as having some level of value and sensitivity, it follows that all information requires security considerations.

1.3. Applicability of this Document

This NPG applies to all NASA employees and NASA contracts (as provided by the terms and conditions of the contract), where appropriate in achieving Agency missions, programs, projects, and institutional requirements. Facilities, resources, and personnel doing work at a college, university, or research establishment under a contract or grant from NASA are included in the applicability of this document to the extent prescribed by the contract or other agreement, specifically as follows:

a. These guidelines will be implemented for any Center IT that is outsourced to 1) another Center; 2) another Government agency; or 3) commercial facilities. All agreements or contracts prepared with the operators of these facilities will contain the controls specified in this document, unless the operator can furnish and certify a superior level of IT security.

b. Generally excluded are contractor or research facility computing and information resources that are not under direct NASA management cognizance or that are merely incidental to a contract (e.g., a contractor`s payroll and personnel system). If these systems are connected as part of a Center`s network, they will be required to follow NASA and Center policies.

c. The provisions of this NPG should be applied in university environments in which NASA is supported through formal agreements, such as grants, cooperative agreements, contracts, and purchase orders. The extent of compliance with this NPG in university environments needs to be evaluated on a case-by-case basis and may range from minimal compliance (e.g., for one-time research activities in which there is not clear indication that NASA is the information owner) to more stringent compliance (i.e., for universities processing NASA-owned information on a long-term basis.)

1.4. Audience for this Document

This document is intended for all NASA civil service and NASA contractor employees who have access to NASA IT resources. Specifically, this document is designed to assist those with assigned IT security responsibilities in this NPG to successfully fulfill those responsibilities.

1.5. Key Elements of the IT Security Program

a. Roles and Responsibilities--Chapter 2 provides a good starting point to understand roles and responsibilities within the IT Security Program. This chapter describes each of the key positions and groups involved in the IT Security Program and the responsibilities for IT security that are assigned to them. As appropriate, it provides cross-references to other chapters that describe how to complete the key tasks assigned to a particular position or group.

b. Metrics--For managers and others responsible for ensuring that key metrics are met, chapter 3 describes what the metric requires, who is responsible for performing each metric, and when or how often each should be accomplished.

c. Program Task--Guidance for completing key tasks within the IT Security Program is found in chapter 4. For each task, such as conducting security planning and conducting penetration testing, the chapter describes who is responsible for the task, what the task requires, and when the task is to be accomplished, and how the task should be accomplished.

d. Documentation--For managers and those who need to prepare and review IT security documentation, chapter 5 describes who is responsible for producing and distributing the documents, what information the document will contain, and how the document will be organized.

e. Baseline Requirements--For those responsible for implementation of the baseline security requirements, appendix A provides the minimum technical, procedural, and physical controls needed for protecting NASA`s IT resources.

1.6. Technical Phrasing and Language

When appropriate, this document uses technical phrasing to describe IT security policies, procedures, requirements, and guidelines. These phrases have special meanings and importance in this document, some of which are identified and defined below.

a. Information Technology (IT) Resources--Data and information, computers, ancillary equipment, software, firmware, and similar products, facilities that house such resources, services, including support services, and related resources used for the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data. Telecommunication systems, network systems, and human resources are included as well. (IT Resources was formally known as Automated Information Resources.)

b. System-- "System" refers to a set of information resources under the same management control that share common functionality and require the same level of security controls.

b.1. The phase "General Support Systems," as used in OMB Circular A-130, Appendix III, is replaced in this document with "system" for easy readability. A "system" includes "Major Applications," as used in OMB Circular A-130, Appendix III, (e.g., payroll and personnel program software, mission control software, or software for command and control of space vehicle). By categorizing both "General Support Systems" and "Major Applications" as "systems" in this document, the procedures and guidance can address both in a simplified manner.

b.2. When writing the required IT Security Plans, two formats are provided--one for General Support Systems, and one for Major Applications. This ensures that the differences for each are addressed.

b.3. A system normally includes hardware, software, information, data, applications, telecommunication systems, network communications systems, and people. A system`s hardware may include desktop systems (e.g., PC`s, Macintoshes, laptops, handheld devices), workstations and servers (e.g.,Unix, NT, NC), local area networks (LAN), and any other platform regardless of the operating system. (See paragraph 4.2.6, "Determine the Scope" for more information.)

c. Special Management Attention--Some systems require "special management attention" to security due to the risk and magnitude of the harm that would result from the loss, misuse, unauthorized access to, or modification of the information in the system. These systems are considered to be the most important for NASA to accomplish its mission. Paragraph 4.2.8 provides more information about these systems, including guidelines for determining which systems require "special management attention." Throughout the rest of this document, "special management attention" will appear within quotation marks to call attention to each reference.

d. Major Application--An application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, unauthorized access to, or modification of the information in the application. All "Major Applications" require "special management attention." The IT Security Plan for a Major Application may be defined broadly enough to include hardware, software, networks, and even facilities where it is reasonable. This permits the systems to be bounded in reasonable ways for the purposes of security planning.

All Federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate.

Figure 1-1

1.7. Authority of this Document

a. Authorization for implementing an IT Security Program is based on the Computer Security Act of 1987, as amended. This law establishes a clear Federal mandate that sensitive information in a computer operated by or on behalf of the U. S. Government will be protected. The Office of Management and Budget (OMB), given the expansion of distributed processing, has provided in Appendix III to OMB Circular A-130 that all systems contain some sensitive information which requires protection.

b. Subsequent Federal and State laws, Presidential Executive Orders (EO), Office of Personnel Management (OPM), OMB, and NASA Policy Directives provide for the substance of the NASA IT Security Program.

c. The description of ways sensitive information will be protected appears in OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources. This OMB document, which applies to all Federal agencies, provides the basic elements of the NASA IT Security Program as reflected in Chapter 4, IT Security Procedures and Guidance. Although NASA has refined these basic elements so that they make sense in a NASA context, all IT security tasks that managers are called upon to perform can be traced to OMB`s guidance.

CHAPTER 2. Information Technology (IT) Security Roles and Responsibilities

The NASA IT Security Program involves all staff in some capacity. NASA Headquarters, Centers, and contractor sites have the latitude to use their internal organizational structure to fulfill the roles and responsibilities described in this chapter provided the approach is documented in policy or guidance.

2.1. Agency Management Roles

2.1.1. NASA Chief Information Officer (CIO)

NASA created the position of CIO to manage IT within the Agency. While maintaining an effective and economical Information Resource Management (IRM) program, the CIO must also ensure that standards and policies for using resources incorporate effective protection measures. A key element of the IRM Program is protecting information resources. To this end, the NASA CIO is responsible for IT security and has the management oversight responsibilities for ensuring the confidentiality, integrity, and availability of information resources. The NASA CIO's responsibilities for ensuring the confidentiality, integrity, and availability of information resources are as follows:

a. Providing advice and assistance to the Administrator and other senior Agency personnel to ensure that Agency IT security goals, priorities, and requirements are effectively and efficiently addressed to protect the Agency's investment in IT resources.

b. Issuing NASA IT security policies, architectures, standards, best practices, and guidance.

c. Appointing Agency representatives to Federal groups concerned with IT security.

d. Appointing a Principal Center for IT Security responsible for developing IT security architectures, standards, best practices, and guidance for the Agency on behalf of the NASA CIO.

2.1.2. Manager of the Principal Center for IT Security (PCITS)

Pursuant to the direction of the CIO, the manager of the PCITS has oversight responsibility for establishing an effective Agencywide IT security management program, maintaining a proactive role in responding to current and new threats, researching IT security, and developing technology to ensure that the Agency can take advantage of the changing computer environment in a secure manner. The manager of the PCITS must ensure that activities at other Principal Centers for IT are implemented in a way that provides security controls. The manager of the PCITS is responsible for the following:

a. Managing and coordinating the overall direction and structure of the NASA IT Security Program.

b. Defining, budgeting, and implementing an Agency IT Security Plan which ensures that applicable management, operational, and technical controls are defined and applied, and their results are measured.

c. Advising and recommending IT security policies, architectures, standards, best practices, and guidance to the NASA CIO and coordinating Agency IT security activities with the other IT Principal Centers to ensure cost-effective integration.

d. Defining, planning, and implementing Agency IT security standards that foster the integrity, confidentiality, and availability of NASA information and technology supporting the Agency's mission, programs, projects, and institutional requirements.

e. Collecting and analyzing metrics quarterly in accordance with NPD 2810, Security of Information Technology, and assisting the NASA CIO in assessing the state of the Agency's IT security posture. (See chapter 3 for descriptions of these metrics.)

f. Establishing an IT Security Working Group and Expert Centers as necessary to assist in implementing Federal and NASA directives, policies, and guidance.

g. Coordinating with other Federal agencies and groups such as the National Institute for Standards and Technology (NIST) and the National Security Agency's Information Systems Security Organization (ISSO) for emerging IT security technology, best practices, and secure solutions.

2.2. Center Management and Key IT Security Roles Within Centers

2.2.1. Center Directors and the Associate Administrator for Headquarters Operations

The Agency's Center Directors and the Associate Administrator for Headquarters Operations have oversight responsibilities for ensuring that an effective Center IT Security Program is established and maintained. These managers must be aware of threats to the Center's missions and the effects that a compromise in the confidentiality, integrity, and availability of information resources could have. A successful Center IT Security Program depends on conducting periodic reviews of the program at the Center directorate level and using metrics to determine the program's status. NASA Center Directors and the Associate Administrator for Headquarters Operations are responsible for the following:

a. Ensuring compliance with Federal, Agency, and Center IT security policies, standards, and practices.

b. Appointing a Center IT Security Manager who will provide organization and direction for implementing the NASA IT Security Program at the Center level. (See paragraph 2.2.4 for a detailed description of the Center IT Security Manager's responsibilities.)

c. Approving a Center IT Security Plan. (See paragraph 5.2 for the organization and content of this plan.)

d. Appointing a Designated Approval Authority (DAA) who will accredit information resources for processing national security information. The DAA must be an individual knowledgeable in computer, telecommunications, and networking technology as well as security methods and practices as set forth in the National Training Standard for Designated Approving Authority, National Telecommunications and Information System Security Instruction (NSTISSI) No. 4012. The DAA should not have a program or project interest in the facility and systems they accredit for processing national security information. The DAA must have the authority to allocate resources to achieve an acceptable level of security, to remedy security deficiencies, or to halt processing. (See paragraph 2.2.5 for a description of the DAA's responsibilities.)

e. Working through the Center/Headquarters CIO: operating and maintaining common technology investments; implementing the requirement for IT Security training of civil service personnel and contractors (incorporation into contracts); ensuring that employees/contractors adhere to IT Security policies and procedures and are held accountable for failure to do so; and determining when IT security incidents are placing NASA's missions, its customers, its reputation, or its assets in jeopardy to a degree that the Center must exercise its responsibility to unilaterally control or terminate incidents. The last activity includes the responsibility to follow the procedures for working with the Office of Inspector General (OIG) and for notifying the OIG before controlling or terminating incidents, whenever possible, as described in paragraph 4.4.9.

2.2.2. Center Chief Information Officer (CIO)

The Center CIO, like the Agency CIO, is responsible for establishing an effective and economical IRM program for his or her Center. The IRM program defines the design and operation of the Center's information infrastructure (such as networks, electronic mail applications, servers, and electronic forms). The Center CIO shall assure IT security is a significant decision factor and appropriately integrated while striving to reduce software, hardware, and maintenance costs and working to increase productivity, interoperability, and functionality. The Center CIO and Organization Computer Security Official can ensure that the user community receives the best balance of performance, cost, and risks by using life-cycle planning in designing IT resources to meet customer requirements. (See paragraph 4.1 for information about IT security in the life-cycle process.) The Center CIO's responsibilities for IT security are as follows:

a. Ensuring that computer architectures, standards, best practices, policies, and guidance contribute to the secure operation of the Center's systems and the protection of the Center's data and information.

b. Ensuring that sufficient resources are budgeted and available to implement and maintain the technical security controls of the Center's IT infrastructure.

c. Assisting the Center IT Security Manager to prepare the annual Center IT Security Plan for Center Director approval. (See paragraph 5.2 for the organization and content of this plan.)

d. Working with the Office of Procurement and Program/Project Managers to include appropriate IT security requirements in specifications and Statements of Work (SOW) for acquiring or operating systems, applications, equipment, software, storing data, and related services. (See paragraph 2.3.4 for the Procurement office's IT security responsibilities.)

e. Ensuring that the computer infrastructure has built-in recovery features (availability), provides adequate baseline protections (confidentiality), and protects data from modifications (integrity).

f. Approving "to process" systems identified as requiring "special management attention".

g. Coordinating with the Center Director, when line managers and the IT Security Manager cannot reach agreement regarding accepting risk and approving a system to process, to make a determination.

2.2.3. Senior Organizational Managers

Senior organizational managers include, but are not limited to, Directorate Chiefs, Division Chiefs, Program Managers, Chief Executive Officer, Chief Financial Officer, and Chief Information Officer. Achieving a sound IT security posture depends on senior organizational managers being involved in and actively supporting IT security planning, budgeting, and training activities within their respective organizations. Senior organizational managers have a practical role in ensuring that "major information systems" identified by OMB Circular A-11, Budget Formulation/Submission Process, and other critical systems and major applications within their organization receive special attention due to the impact a compromise or failure would have. (See paragraph 4.2.8 for information on systems requiring "special management attention.") A senior organizational manager's responsibilities for IT security are as follows:

a. Appointing a Computer Security Official (CSO) for his or her organization who is knowledgeable of the organization's information, data, and the mission security requirements. The CSO needs to be cognizant of the organization's programs, projects, sensitive data, and systems, to understand their value and importance to NASA, and to be competent to oversee the implementation of IT security for the organization and influence budgets and schedules to reduce risk as necessary. (See paragraph 2.2.6 for a description of the CSO's responsibilities.)

b. Ensuring that the security risks of systems requiring "special management attention" under their cognizance are identified, that risk assessments are accomplished, that contingency planning is documented and tested, and that adequate safeguards are implemented consistent with the determination of acceptable risk. (See paragraph 4.2.8 for information about systems requiring "special management attention.")

c. Certifying the adequacy and appropriateness of security controls before placing into operation a system requiring "special management attention." Also, periodically recertifying systems throughout their life cycle.

2.2.4. Center IT Security Manager

The Center IT Security Manager is responsible for the Center IT Security Program. The Center IT Security Manager's role is to develop Centerwide IT security policies and guidance, to provide computer awareness and training, to maintain an incident response capability, and to document, review, and report the status of the Center IT Security Program. The Center IT Security Manager's responsibilities for IT security include the following:

a. Developing and issuing directives necessary to implement the Center's IT Security Program.

b. Developing, implementing, and monitoring the Center's IT Security Plan.

c. Ensuring that line managers identify systems requiring "special management attention" and that senior organizational managers are aware of their special oversight responsibilities. (See paragraph 4.2.8 for information on systems requiring "special management attention.")

d. Supporting and coordinating with the training office to develop a Center IT Security Awareness and Training Plan for implementing a training program that adheres to Agency initiatives and direction for IT security awareness and training. The Center IT Security Awareness and Training Plan will ensure that the Center's user community has the awareness, knowledge, and skills necessary to protect NASA information, data, and systems. This plan will become part of the Center's Training Plan.

e. Establishing a process to ensure that appropriate screening has been completed for individuals requesting system privileges and that these individuals are eligible to be issued accounts. (See paragraph 4.5 for information on privileges and personnel screening.)

f. Conducting periodic reviews and compliance checks to ensure the following:

(1) IT Security Plans are current or planned.

(2) Significant changes to hardware, software, or operating environments are analyzed and documented for risk impact.

(3) Center IT security policies and guidelines are current and comply with Federal and NASA regulations.

(4) IT Security Plans are performed at least once every 3 years or upon significant modifications.

g. Maintaining documentation on IT Security Plans and significant IT security incidents, audits, and evaluations, as well as establishing procedures for reporting metrics to management.

h. Coordinating with the Center Chief of Security (CCS), local OIG, and other IT security response teams to gather intelligence data regarding threats, concerns, and hacker techniques affecting the vulnerability of NASA information and systems. (The IT Security Manager will require a security clearance to receive classified intelligence data.)

i. Providing necessary utilities and training to the organizational CSO's and System Administrators to ensure that they can purge nonreleasable data or information from storage media prior to their release.

j. Responding appropriately to IT security incidents by doing the following:

(1) Organizing and directing inquiries, examinations, and corrective actions.

(2) Establishing and maintaining a technically oriented IT security incident response team.

(3) Reporting incidents to Center and Agency management to include the PCITS and the Expert
Center for IT Security Notification, Incident Coordination and Response.

(4) Reporting incidents to the OIG per the procedures described in paragraph 4.4.9.

k. Coordinating incidents involving criminal activities with the local OIG.

l. Conducting penetration testing to ensure that controls are effective. (See paragraph 4.6.6.)

m. Providing self-inspection IT Security guidance to System Administrators.

n. Conducting periodic reviews of the adequacy of the safeguards for operational, accredited systems requiring "special management attention." To the extent possible, these reviews should be conducted by persons who are independent of the user organization and of the Automated Information System (AIS) operation or facility.

2.2.5. Designated Approval Authority (DAA)

Each Agency Center Director and the Associate Administrator for Headquarters Operations appoints a DAA for that Center. The DAA is responsible for accrediting information resources that process national security information (i.e., classified information). By accrediting a system, the DAA formally assumes responsibility for the operation of the system within a specified environment. The DAA must have the authority to allocate resources to achieve an acceptable level of security and to remedy security deficiencies or to halt processing. The accreditation decision indicates that due care has been taken to balance security requirements, the mission, and resources against a defined risk. The DAA's responsibilities for IT security are as follows:

a. Accrediting Center-owned IT systems that process national security information and that have been certified by the data owner, the facility manager, the Center IT Security Manager, and the CCS.

b. Working closely with the Center IT Security Manager, the CCS, and the OIG to ensure an awareness and understanding of current threats and vulnerabilities.

c. Developing processes for documenting the security posture of systems, for certifying the accuracy of supporting documentation, for reviewing systems' security controls, for testing these security controls, and for granting accreditation to process.

2.2.6. Organizational Computer Security Official (CSO)

An organizational CSO is responsible for a particular organization's IT Security Program. The organizational CSO serves as the critical communication link to and from that organization for all IT security matters. The organizational CSO's responsibilities for IT security are as follows:

a. Establishing management controls and a communications process to ensure that the organization's implementation of IT security is consistent with mission needs and NASA policies and guidance.

b. Identifying to the Center IT Security Manager any systems that require "special management attention." (See paragraph 4.2.8 for information about systems requiring "special management attention.")

c. Serving as the organization's representative to the Center IT Security Manager and representing the organization's line managers on security matters. (See paragraph 2.2.7 for the responsibilities of line managers.)

d. Reporting suspected and actual IT security incidents to the Center IT Security Manager and line management. (See paragraph 4.4 for information on handling security incidents.)

e. Establishing a process to ensure that the organization's storage media are purged of any data or information that has not been approved for public release prior to releasing the media outside the organization's control. (This includes releases for repair, replacement, or upgrade as well as excessing.)

f. Reporting periodically to the Center IT Security Manager and the organization's senior manager on the status of the organization's IT security posture.

g. Identifying an alternate CSO.

h. Reviewing annually the IT Security Plans for the organization's systems. (Paragraph 4.2 provides information on security planning, and paragraph 5.1 describes the organization and content of IT Security Plans.)

i. Ensuring that IT Security Plans are protected as "For Official Use Only" material when system vulnerabilities are disclosed. (See NPG 1620, Security Procedures and Guideline, chapter 4)

2.2.7. Line Manager

2.2.7.1. Every system requires a civil service line manager who is responsible for ensuring that the system or application performs as designed and meets the needs of customers and data owners. If a system or application is operated and managed by contractors, these contractors must report to a civil service line manager. Typically, a line manager is at the branch or division level.

2.2.7.2. IT security plays a significant role in ensuring that customers' expectations for performance, confidentiality, integrity, and availability are met. To meet these expectations, line managers must conduct risk assessments, implement protective controls, test controls, and test contingency plans. (See paragraph 4.2.10 for information on risk assessments.)

2.2.7.3. The line manager has the following responsibilities for IT security:

a. Identifying to the organizational Computer Security Official and the Center IT Security Manager any systems requiring "special management attention." (See paragraph 4.2.8 for information about systems requiring "special management attention.")

b. Ensuring that the security risks of systems under their cognizance are identified and evaluated and that adequate safeguards are implemented consistent with the estimated value of the information processed and acceptable risk levels.

c. Certifying the adequacy and appropriateness of security controls before putting new systems into operation. Also, periodically conducting the same certification throughout the life cycle of the system or application. (See paragraph 3.1.4 for information on obtaining authorization to process.)

d. Developing and implementing IT Security Plans for assigned systems and periodically testing the contingency operations associated with these plans. (Paragraph 3.1.2 provides more information on the requirement for IT Security Plans, and paragraph 5.1 describes the organization and content of IT Security Plans. Paragraph 4.2 provides information on IT security planning, and paragraph 5.3 provides the organization and content of IT Security Contingency Plans.)

e. Ensuring that a properly trained System Administrator is assigned as the focal point for the security of each system or application. (See paragraph 2.2.8 for the responsibilities of the System Administrator.)

f. Reporting suspected IT security incidents to the Center IT Security Manager, organizational CSO, and their line management. (See paragraph 4.4 for guidance on reporting and handling security incidents.)

g. Ensuring that individuals assigned to positions requiring system privileges are screened appropriately. (See paragraph 4.5 for information on how to request security investigations for individuals who require special privileges.)

h. Ensuring that IT Security Plans are protected as "For Official Use Only" material when system vulnerabilities are disclosed. (See NPG 1620, Security Procedures and Guideline, chapter 4.)

2.2.8. System Administrator or System Security Administrator

2.2.8.1. Each system will have a System Administrator who will ensure that the protective security measures of the system are functional and who will maintain its security posture. Depending on the complexity and security needs of a system or application, the System Administrator may have a designated System Security Administrator who will assume security responsibilities. (See Figure 2-1) Although line managers are accountable for the operation and security of systems, System Administrators usually do the hands-on operational and security work.

The remainder of this document uses the term "System Administrator" even though the person with the responsibilities described below might have the title of

Figure 2-1

2.2.8.2 The System Administrator, whether a civil service or contractor employee, is responsible for the following:

a. Making sure that all users complete an Account Request Document approved by a Government management official responsible for the individual (e.g., manager, sponsor, task manager) for all user accounts and that the information gathered is handled in accordance with the Privacy Act.

b. Promptly disabling access to a user's account if the user is identified as having left the Center, changed assignments, changed contracts, or completed work on a grant or other agreement, or is no longer requiring system access. Written authorization will be required from the Government management official, who originally authorized the account, to reactivate the user's account. (Digitally signed e-mail is acceptable).

c. Granting accounts only to individuals who have had the appropriate personnel screening. The Center IT Security Manager will provide a process for verifying that appropriate screening has been completed and that the individual is eligible to be issued an account. (See paragraph 4.5 for information on personnel screening and paragraph 4.7 for guidance on granting access to systems.)

d. Granting accounts to foreign nationals without permanent resident alien status only with prior approval by the CCS. (See paragraph 4.7.6 for guidance on granting foreign nationals access to systems.)

e. Performing annual self-inspections of their systems and reporting the findings to their line managers and the cognizant organizational CSO or designee. The Center IT Security Manager will provide guidance for conducting self-inspections.

f. Reporting IT security incidents. (See paragraph 4.4 for guidance on reporting IT security incidents.)

g. In response to an IT security incident, taking necessary actions to prevent further damage to their systems and documenting their actions. (See paragraph 4.4 for guidance on handling IT security incidents.)

h. Identifying personnel who will be responsible for systems if an IT security incident requiring immediate attention occurs when the System Administrator is absent. The names and contact information for these personnel will be provided to their management and their organizational CSO.

i. Periodically using tools to verify and/or monitor compliance to password guidelines. (See paragraph A.6.3 in the appendix for the baseline requirements concerning passwords.)

j. Using IT security tools to assist in detecting modifications to the system and monitoring audit logs.

k. Ensuring that security controls are in place and functioning.

2.2.9. Center Information Processing Service Organization (IPSO)

2.2.9.1. Center IPSO's are organizations and groups that provide computer-related services. IPSO's provide services
such as business systems, electronic mail, electronic forms, applications servers, telecommunications, local and wide area networks, data storage, scientific computing resources, and desktop services. Managers of IPSO's must complete IT Security Plans for their systems and ensure that major applications requiring "special management attention" have IT
Security Plans.

2.2.9.2. A fundamental security objective of each service provider will be to ensure that customer security requirements are identified and that appropriate technical and operational controls are provided. To achieve this objective, each IPSO is responsible for the following:

a. Establishing a baseline of security standards for each functional service provided.

b. Ensuring that reasonable controls are in place to protect the networking environment, both internally and externally to the Center.

c. Providing assistance to programs and projects that need to apply additional security controls to ensure adequate protection for their mission objectives.

d. Ensuring that personnel working in sensitive positions have been identified and that background screening is done to ensure personal integrity. (See paragraph 4.5 for information on personnel screening.)

e. Ensuring that systems requiring "special management attention" are identified and certified prior to bringing them on line. (See paragraph 4.2.8 for information on systems requiring "special management attention.")

f. Ensuring that all IPSO support personnel, including both Government and contractor staff, receive initial and follow-on IT security training.

2.3. Center Support Roles

2.3.1. Center Chief of Security (CCS)

The CCS has the following responsibilities for IT security:

a. Providing oversight, guidance, and approval authority for projects conducting classified activities.

b. Conducting appropriate personnel security screening for those working in sensitive positions and those who can bypass IT technical security controls and processes. (See paragraph 4.5 for information on personnel security investigations.)

c. Coordinating, investigating, and approving requests for foreign nationals who require access to systems, applications, and networks operated by or on behalf of NASA.

d. Developing a process to gather intelligence information regarding threats towards IT resources and providing this information to the Center IT Security Manager and the CIO. Intelligence information includes specific categories of information; methods being used to gather restricted information; specific sites, persons, or countries conducting hostile activities towards the United States or NASA; and successful counter measures.

e. Ensuring the physical security of Center IT resource facilities.

f. Developing policies and procedures for protecting national security information (i.e., classified information).

g. Providing oversight for all facilities that the DAA has authorized to process and handle national security information.

h. Investigating all potential compromises of national security information with the assistance of the Center IT Security Manager, as required, and notifying the cognizant agencies as necessary. The CCS needs to coordinate with the local OIG regarding the criminal aspects of the investigations.

i. Establishing and overseeing a Center process that will ensure that all classified processing is coordinated with the Center IT Security Manager.

j. Conducting, with the assistance of the IT Security Manager, preliminary inquiries into IT security incidents. Preliminary inquiries may include contacting external groups and other organizations to better understand the threat posed by incidents, to share information concerning incidents, and to develop recommendations for Center management regarding the best course of action in dealing with incidents.

k. Coordinating with the Center IT Security Manager, local OIG, and other IT security response teams in the investigations of IT security incidents. The CCS will involve other law enforcement agencies, if the situation warrants.

2.3.2. Training Office

Numerous public laws and Federal agency standards define the need and requirements for mandatory and continuous IT security awareness and training. (See paragraph 4.3.1.) To ensure that these laws and standards are adhered to and that reasonable protection is provided, all Government agencies are required to establish an IT Security Awareness and Training Plan. This plan must address the needs and requirements of those who have IT security responsibilities, both civil service personnel and contractors. A Center's training office is assigned the following IT security responsibilities:

a. Coordinating with the IT Security Manager to develop a Center IT Security Awareness and Training Plan to ensure that the Center's user community has the awareness, knowledge, and skills necessary to protect NASA information, data, and systems. This plan will become part of the Center's training plan.

b. Working with the Center IT Security Manager in the following:

(1) Developing an IT Security Awareness and Training Plan.

(2) Identifying requirements for IT security awareness and training.

(3) Identifying sources for providing the training.

(4) Budgeting funds for both initial and follow-on IT security curricula.

(5) Maintaining records that show who has received IT security training.

2.3.3. IT Security Incident Response Team

When an IT security incident occurs or is suspected, Centers need the ability to respond. To meet this need, the Center IT Security Manager is responsible for identifying a response capability to take appropriate actions. This response capability should leverage existing expertise depending on the nature of the incident. The team should be comprised of individuals with the skills necessary to analyze the compromised system's operating system and hardware, specific applications on the system, and network connections, as well as to deal with management issues relating to risk, cost, and performance. The response capability can be in formal or informal teams. Response teams are responsible for the following:

a. Exercising caution to keep information within prescribed channels. Failure to do so may impede or even preclude the Government's chance of obtaining a conviction if a crime is discovered or may cause needless embarrassment to others if what seems at first to be a crime later proves otherwise. Electronic communications regarding incidents will be conducted in a secure manner through the use of secure messaging technology (e.g., encryption). (See paragraph 4.4 for information on security incidents.)

b. Keeping the Center IT Security Manager updated on the status.

c. Determining if an incident has occurred.

d. Ascertaining the details.

e. Limiting further damage.

f. Determining the initial impact.

g. Preserving evidence (Check with the Center IT Security Manager and OIG for guidance and questions).

h. Assisting System Administrators in restoring and testing the restored system.

i. Recommending actions to line managers and data owners.

j. Documenting all actions taken.

k. Developing a recovery plan.

2.3.4. Procurement Office

2.3.4.1. The Procurement office's role in IT security is to ensure that contracts and grants for hardware, software, data management, and support services comply with Center IRM and IT security policies, procedures, and guidelines. Modifying hardware, software, and service contracts to meet requirements is costly. By working closely with the Center CIO and the Center IT Security Manager and by developing specific contract clauses, the Procurement office helps the Center maintain its interoperability, computer infrastructure, and security posture.

2.3.4.2. The Procurement office, working with the Center CIO and the Center IT Security Manager, is responsible for the following:

a. Identifying acquisitions for computer hardware, software, data management, and support services.

b. Establishing a joint process with the Center CIO and IT Security Manager to review acquisitions for IT security issues and concerns.

c. Ensuring that all procurement actions, including solicitations and contracts, comply properly with IT security policies, procedures, and guidance.

2.3.5. Office of Inspector General (OIG)

The OIG's role in IT security is to investigate computer crimes for possible prosecution in court and to conduct reviews of IT resources for proper management, which includes appropriate protective controls. In this role, the OIG agrees that it will perform the following:

a. Promptly notify appropriate NASA management of incidents whenever the OIG has reason to believe, or is aware, that the incidents may pose a threat to human safety or critical missions.

b. Coordinate, to the extent practicable, with the Center IT Security Manager or Center management, when use of Center computer or network data is needed to support an investigation being conducted by the OIG.

c. Investigate, as appropriate, incidents forwarded by the Center IT Security Managers which constitute a computer crime, as described in paragraph 4.4.9.

d. Serve as the focal point for referrals to the Department of Justice and other external law enforcement organizations of all violations of Federal criminal and civil statutes related to computer system intrusions or criminal misuse of computers.

2.4. Customer Roles

2.4.1. Project and Program Managers

Major activities usually have project or program managers assigned to them at their initiation to lead them throughout their life cycle. Integrating IT security into the program management requirements of NPG 7120.5 is necessary to ensure that IT security is addressed early in the process. Project and program managers play a key role in ensuring that security requirements are identified during the concept phase, addressed throughout design reviews, tested during implementation and operational phases, and maintained during the disposal process. (See paragraph 4.1 for information on the life- cycle process). Project and program managers have the oversight responsibilities for the following:

a. Including IT security as part of the operational and technical design.

b. Defining the potential impact that could result from an IT security incident.

c. Coordinating with Center IT Security Manager on threats and vulnerabilities.

d. Conducting an initial risk assessment and analysis.

e. Selecting risk-reduction controls.

f. Establishing a contingency plan.

g. Publishing an IT Security Plan.

h. Ensuring that systems are authorized for processing by line managers and data owners.

2.4.2. Data Owners

All data have an owning organization responsible for its confidentiality, integrity, and availability. Although data owners may have their information processed by another organization or contractor, they are responsible for understanding any risk that another line manager has accepted for the system that processes their data. Data owners have the following responsibilities for IT security:

a. Coordinating with line managers, who have a shared responsibility for protecting NASA information, to ensure that each understands the risk accepted by the other. If a data owner cannot accept the risk posed by the system that processes his or her data, the data owner must find another means to process these data. Sometimes this may mean acquiring dedicated resources or paying to upgrade the existing system to reduce the risk to an acceptable level.

b. Identifying their data, its value, and its importance to NASA (i.e., impact if lost).

c. Ensuring that adequate controls are applied to protect their data.

d. Publishing an IT Security Plan, if the security of their data is not addressed in the IT Security Plan for the system that processes their data. (Data owners should work with the system's line managers or project/program managers to complete the plan. See paragraph 4.2 for information on IT security planning and paragraph 5.1 for the content and organization of IT Security Plans.)

e. Working with line managers or project/program managers to authorize processing.

f. Continually evaluating security controls to ensure adequate protection of data.

2.4.3. User Community and NASA Customers

Because NASA resources, information, data, and processing systems are held in public trust, the NASA user community and NASA customers all share responsibility for protecting these IT resources. Policies and guidance cannot always be implemented through technical controls. Consequently, individuals are relied on to voluntarily comply with procedures. The user community and customers will be made aware of the procedures they must follow. All users of data, systems, and applications have the following responsibilities for IT security:

a. Knowing the liability issues for handling, distributing, and protecting the data they use, control, and access.

b. Being familiar with policies, guidance, and procedures for using the data, systems, and software applications to which they have been granted access. (See paragraph 4.8 for policies on using Government IT resources.)

c. Understanding Agency and Center policies regarding "Proper Use" and "Expectation of Privacy." (See paragraph 4.8 for policies on the appropriate use of Government IT resources and paragraph 4.10 for information on privacy.)

d. Complying with Center IT policies and guidance and systems' rules of use.

e. Reporting incidents or suspected incidents to their System Administrator, line manager, organization CSO, or Center IT Security Manager. (See paragraph 4.4 for guidance on reporting security incidents.)

CHAPTER 3. Information Technology (IT) Security Program Metrics

The Agency has established a set of metrics to measure its compliance with the basic elements of the Computer Security Act and OMB Circular A-130, Appendix III. These metrics address whether key security requirements for a system have been met according to policies, procedures, and guidance. The metrics provide managers with a high-level status of their IT Security Program, insight into areas of noncompliance, and tools to measure improvement. Although the metrics indicate whether a requirement has been met, they do not validate the quality of the program. Managers with oversight responsibility must understand the processes and methodology behind the metrics. This chapter identifies these metrics and provides high-level descriptions of them. As appropriate, this chapter refers to other parts of this document, which provide details on ways to accomplish each metric.

3.1. Metrics Table

The following table identifies the responsible person for completing a metric and indicates when or how often these items need to be rechecked. (See Figure 3-1.) Although these metrics seem to be a simple set of requirements, each requirement consists of a set of tasks that, when completed, help ensure an acceptable level of security. Detailed descriptions of each of these requirements follow.

Metric	Who is Responsible	When/How Often
Assignment of responsibility	Line manager	Before the system goes online
IT Security Plans	Line manager	Every 3 years or upon significant change
Periodic reviews	Line manager	Every 3 years or upon significant change
Authorization to process	Line manager	Every 3 years or upon significant change
System documentation reviews	Organization Computer Security Official	At least annually
IT Security Awareness and Training Plan	Center Training Office	At least annually
IT Security Incident Reports	Center IT Security Manager	Quarterly

Figure 3-1

3.2. Assignment of Responsibility

Every system will have someone identified as being responsible for its security. This person, who will be referred to as the System Administrator (or System Security Administrator), may be a civil service or contractor employee as provided by the terms and conditions of the contract. The System Administrator must know the nature of the information processed by the system (or an application on the system) and be able to apply and manage appropriate security controls. The line manager for the system or application appoints the System Administrator. The appointment must be in writing and given to both the individual appointed and the organizational CSO, who will report the appointment to the Center IT Security Manager. The appointment remains in effect until the line manager assigns the responsibility to someone else.

3.3. Information Technology Security Plan

Every system will have an IT Security Plan that documents its security posture at a particular point in time. The line manager for the system or application is responsible for completing this document. The IT Security Plan reports the outcome of the IT security planning process, which is described in paragraph 4.2. An outline of the contents and organization of an IT Security Plan appears in paragraph 5.1. IT Security Plans are considered sensitive documents and must be protected as such. They must be available to the Center IT Security Manager, organizational CSO, the line manager`s own management, certifying officials such as data owners, and authorized external auditors as required. An IT Security Plan remains in effect until a new one is issued; however, the maximum time that may elapse before issuing a new plan is 3 years.

3.4. Periodic Reviews

Periodic reviews of security controls are required to ensure that security is maintained as the system is changed and upgraded; as better technology is used; and as people, procedures, and risks change. The scope and frequency of reviews depends on whether the system requires "special management attention," its operational environment (e.g., dynamic or steady), and the degree of risk that is considered acceptable. (See paragraph 4.2.8 for more information about systems that require "special management attention.") Periodic reviews for each system include the following:

a. The security controls for each system will be reviewed every 3 years or upon significant change, whichever comes first. The line manager will retain any documentation generated as a result of the review and attach it to the IT Security Plan.

b. The line manager will report the results of the reviews to the organizational CSO, who will in turn report the significant changes to the Center IT Security Manager. If the periodic review indicates that the system has changed so much that the current IT Security Plan no longer describes the system, the IT Security Plan must be updated and reissued.

c. Additional security controls will be implemented if the review indicates that they are required and the risks are unacceptable; the line manager will take the necessary steps to implement them and will update the IT Security Plan accordingly.

3.5. Authorization to Process

Giving authorization "to process" should not be taken lightly. By signing the certification to authorize processing, a line manager is accepting responsibility for the level of risk inherent in the system. An authorization to process may be granted by a separate memo or be integrated into the system`s or application`s IT Security Plan. However, the date that authorization to process was granted must be submitted to the organizational CSO, who will inform the Center IT Security Manager of this date. Before a new or significantly changed system or application can become operational, the appropriate line manager must do the following:

a. Ensure that the IT Security Plan for the system is being followed.

b. Authorize in writing that the use of the system, based on its IT Security Plan, presents an acceptable level of risk to the system and the information it processes.

c. Re-authorize every 3 years or upon significant change, whichever comes first and maintain a copy of the written authorization to process with the IT Security Plan.

3.6. System Documentation Reviews

At least annually, organizational CSO`s are required to review the documentation for the systems that are under the control of their organizations. The purpose of these reviews is to ensure that significant changes are brought to management`s attention and that any necessary corrective actions are planned, budgeted for, and implemented. If there have been no significant changes in the last year, the organizational CSO should report this to the Center IT Security Manager. If changes are in progress, the organizational CSO should advise the Center IT Security Manager and provide a schedule for completing these changes.

3.7. Awareness and Training

Providing civil service and contractor employees with IT security awareness and training is essential in ensuring that they have the knowledge and skills necessary to protect NASA information, data, and systems. The Center IT Security Manager and the Training Office will develop a Center IT Security Awareness and Training Plan to ensure that the Center`s user community has the awareness, knowledge, and skills necessary to protect NASA information, data, and systems. This plan will become part of the Center`s Training Plan. (See paragraph 4.3 for guidance in developing the plan.)

3.8. Incident Reporting and Response

No matter how efficient and effective an IT Security Program is, incidents will occur and procedures and guidance need to be established for recognizing, responding to, and reporting incidents. The Center IT Security Manager bears primary responsibility for responding to IT security incidents and ensuring that they are handled according to the guidelines in this document. The Center IT Security Manager is responsible for reporting metrics on incidents quarterly to the PCITS.

CHAPTER 4. Information Technology (IT) Security Procedures and Guidance

At the core of the NASA IT Security Program are procedures and guidance that need to be followed in order to assess and manage risks. These procedures and guidance provide the tools to ensure that the program's objectives are met and that a level of quality is established. The objectives of the procedures and guidance are to protect the confidentiality, integrity, and availability of information relative to its value. This chapter also identifies who is responsible for completing procedures and describes why these procedures are an important part of the NASA IT Security Program. As necessary, this chapter refers to other chapters for related information. The key security procedures and guidance described in this chapter are the following:

a. IT Security in the Life-Cycle Process.

b. IT Security Planning.

c. IT Security Awareness and Training.

d. Reporting and Handling IT Security Incidents.

e. Personnel Screening.

f. Penetration Testing.

g. Granting Access.

h. Appropriate Use of IT Resources.

i. Software Usage.

j. Access Warning Banner, Notification of Rights, and Monitoring.

k. Use of Encryption Technology.

l. National Security Information.

4.1. IT Security in the Life-Cycle Process

4.1.1. Overview

Security is vital to preserving NASA's investments in IT resources. Since it is not possible to consider and apply security concepts and measures randomly and still maintain an acceptable level of security, security should be included throughout the life-cycle process, from inception through retirement from service. The NPG 7120.5A, NASA Program and Project Management Process and Requirements, provides the basic processes and requirements for the life cycle of all programs and projects. The paragraphs that follow describe how to include security throughout this life-cycle process. Although the model described is generic and may not follow exactly the life-cycle process used by all organizations, this model demonstrates that every milestone in the life-cycle process has a corresponding security component.

4.1.2. The Life-Cycle Process

The life-cycle process spans the entire time that a project/ program is being planned, designed, developed, procured, installed, used, and retired from service.

4.1.3. Security Responsibility in the Life-Cycle Process

The project/program manager is responsible for ensuring that security concerns are included in the life-cycle planning process. Although the manager has this responsibility, other staff members involved in developing, operating, and maintaining systems are responsible for factoring security concerns into the work they do and the decisions they make. These staff members include application developers, system designers, System Administrators, application managers, and System Security Administrators.

4.1.4. Relationship Between the Life-Cycle Process and IT Security Planning

IT security planning is closely aligned to the life cycle of a project or program. Many of the tasks described in this paragraph correlate to IT security planning tasks (such as assessing risk and selecting controls). When a security task has a related task in IT security planning, a cross-reference to the appropriate IT security planning paragraph is provided. The paragraphs for IT security planning describe the way to complete some of the key security tasks in this section

4.1.5. The Life-Cycle Process Phases

Each phase consists of a set of project tasks. For each project task, a corresponding security task should be completed. The paragraphs that follow describe both the tasks for each phase in the life cycle of a project and the corresponding security tasks that should be taken. The life-cycle process consists of the following phases:

a. Project initiation.

b. Project definition.

c. Design.

d. Construction.

e. Installation, integration, and testing.

f. Operations.

g. Upgrade.

h. Disposal of assets at the end of their useful lives.

4.1.6. Project Initiation

Project Task	**Corresponding Security Task**
Identify user needs: □ Identify mission, resources, and priority. □ Describe basic requirements and objectives. □ Provide a general statement concerning the nature of the service requested and overall concept.	Identify security needs: □ Identify the kinds and sensitivity of information that will be stored, processed, or transmitted. (See paragraphs 4.2.8 and 4.2.9 for more information.) □ Identify basic security objectives and goals. □ Identify the security resources needed to manage security.
Evaluate alternatives to satisfy requirements: □ Identify alternatives to satisfy requirements. □ Analyze technical, operational, and economic feasibility. □ Consider costs versus benefits.	Identify security alternatives for each requirement by performing an initial risk assessment: □ Identify threats, vulnerabilities, and risks. □ Analyze technical, operational, and procedural controls for their economic feasibility as project security alternatives. □ Estimate security-related costs versus benefits. See paragraph 4.2.10 for guidance on completing these steps.
Select and approve one approach, establish project objectives, and provide a general definition of the requirement and system or application architecture.	Identify the basic security framework in the selected alternative and provide essential vulnerability information with impact issues and concerns.

4.1.7. Project Definition

Project Task	**Corresponding Security Task**
Prepare a project plan to guide the development effort, budget, and schedules. Include methods for design, coding, documentation, problem reporting, and configuration management in addition to verification, validation, and testing.	Establish security checkpoints in the project plan. These checkpoints include quality assurance for development of security controls, identification of configuration and change control process, and development of an internal audit plan.
Develop a basis for design from user requirements (i.e., functional requirements).	Define security requirements by doing the following: □ Identify new threats, vulnerabilities, and risks. □ Identify user requirements for protecting data. Determine where security requirements apply in the system. □ Determine the mix of security controls. The appendix lists the baseline requirements that the system or application should meet.
Develop preliminary test plans.	Refine the risk analysis and develop a contingency plan. (See paragraph 5.3 for information on contingency plans.) Develop preliminary security test plans that do the following: □ Describe the security objectives (i.e., goals), policies, and requirements. □ Identify the resources needed to test the plan and establish a test schedule. □ Describe evaluation criteria and areas to be tested.

Select an acquisition strategy that is commensurate with cost, risk, and need.	Design requests for proposals (RFP's) and contracts to include security requirements. Design solicitations to provide quality assurance of security controls. Evaluate offers for addressing the adequacy of security controls.
Update requirements analysis and formalize the requirements into a functional baseline.	Include security requirements in the formal functional baseline.

4.1.8. Design

Project Task	**Corresponding Security Task**
Develop a detailed design and supporting specifications for the project, including requirements for input, output, files, databases, and system controls.	Define security specifications, including identification of the following: □ System/subsystem and interface security specifications. □ Program, database, hardware/firmware, and network security specifications.
Develop and update verification, validation, and testing goals and plans.	Update the security test plan and develop a security test procedure. Determine that the procedure will test security specifications and performance under both normal and abnormal circumstances.
Design a solution that satisfies requirements and constraints, and establish a formal functional baseline.	Include security specifications in the formal functional baseline.

4.1.9. Construction

Project Task	**Corresponding Security Task**

Construct the system or application from detailed design specifications.	Develop security code, control access to security code, and identify and document security code, as appropriate to the project.
Perform unit tests and evaluate the results.	Perform unit tests and evaluate security-related code, as appropriate to the project.
Implement a detailed design that results in a system ready for installation. Establish as the formal developmental baseline.	Include approved security components in the formal developmental baseline.

4.1.10. Installation, Integration, and Testing

Project Task	**Corresponding Security Task**
Test system components.	Conduct tests of security in the configured components.
Validate system performance.	Conduct security tests in the integrated system, including assessing functional operation and performance and identifying any test failures. Analyze test results against security requirements.
Install the system with any necessary code modifications.	Install security code with any necessary code modifications, as appropriate to the project.
Prepare users' guides and operations/maintenance manuals.	Prepare documentation of security controls for users' guides and operations/maintenance manuals.
Perform an acceptance test and validate the results.	Conduct an acceptance test and evaluate project security. This testing includes the following: □ An assessment of the functional operation, performance, and resistance to penetrations.

	□ Identification of the level and type of security controls. (See paragraph 4.6 for information on penetration testing.)
Accept the system and establish a formal product baseline.	Verify the project security, identify strengths and limitations, and prepare the required IT Security Plan and supporting documentation. (See paragraph 5.1 for the organization and content of an IT Security Plan.)

4.1.11. Operations

The following security tasks are part of the IT security metrics described in chapter 3. There are security tasks to be accomplished before the system goes into operation and during the operational phase.

4.1.11.1. Before the Operational Phase

Before the system goes into operation, the project manager will ensure that the following have been done:

a. A line manager is assigned responsibility for the IT security of the system.

b. An IT Security Plan is written (see paragraph 5.1 for the organization and content of this plan).

c. The system has been authorized in writing and approved for processing, which signifies the project manager's acceptance of risk.

4.1.11.2. During the Operational Phase

During the operational phase, which could span months or years, the line manager will do the following:

a. Ensure that security is carried out as described in the IT Security Plan.

b. Review the security controls for the system or application at least every 3 years or upon significant change to the system, whichever comes first.

c. Re-authorize processing before the operation of the system or application can continue. This re-authorization signifies the line manager's acceptance of risk.

d. Establish metrics to measure the effectiveness of the IT security controls of the program or project.

4.1.12. Upgrade

4.1.12.1. A system upgrade may result in a significant change to the system configuration and security controls. Examples of significant changes include, but are not limited to, relocation to other facilities, major modification of the existing facilities, introduction of new equipment, addition or deletion of external interfaces, changes to system network connectivity, installation of new operating system software, patches to applications, new releases of software, installation of new application software, introduction of more sensitive data, or a substantial change to the system's risk posture that might affect others on the same network.

4.1.12.2. If a significant change occurs before the next scheduled 3-year review, the line manager must ensure that knowledgeable officials conduct a review of the security controls and re-authorize processing. Results from the review should be documented and attached to the IT Security Plan.

4.1.13. Disposal of Assets at the End of their Useful Lives

4.1.13.1. Once the system or application becomes obsolete and is to be disposed of, the line manager should notify the Center IT Security Manager through the Organization Computer Security Official. (See NPG 1441.1C, Records Retention Schedules, for retention requirements and procedures for specific data and information that needs to be retained.) Current Federal regulations permit giving surplus IT equipment to organizations outside the NASA community. Other organizations are not authorized to possess copyrighted software licensed to NASA or restricted information (e.g., information whose distribution is controlled) that may be stored on NASA's surplus media.

4.1.13.2. Releasing copyrighted software or restricted information outside of NASA, even accidentally, may expose the offending line manager and the Government to considerable liability. Before disposing of any storage media, the line manager must do the following:

a. Ensure that all software and information with release restrictions are erased by overwriting the media at least once. (See Figure 4-1.) If you have any questions concerning releasing information, data, or software on obsolete storage media, erase the media before releasing it for disposal.

b. Ensure that media which do not permit overwriting is destroyed or transferred to another authorized user within NASA.

Deleting information and erasing information are very different. Deleting

usually removes only pointers to the files that contain the information. The information remains on the medium and may often be recovered using widely available software tools. Erasing overwrites the data fields so that the information is truly gone.

Figure 4-1

4.2. IT Security Planning

4.2.1. Overview

This section presents a structured approach for conducting a risk assessment, for analyzing the risk, and for using the results to prepare an IT Security Plan. This process is known as "risk management." IT security planning is the cornerstone of the NASA IT Security Program. Many of the other security tasks described in this chapter (e.g., conducting a risk assessment, contingency planning, and training) are addressed in the IT security planning process or support the plan in some way. For example, security planning parallels many activities in the life cycle process.

4.2.2. IT Security Planning

IT security planning is a methodology for assessing risks, determining an acceptable level of risk, documenting the results of risk assessment, identifying security measures that should be implemented to mitigate risk, and monitoring risks in the environment on an ongoing basis.

4.2.3. Responsibility for IT Security Planning

The assigned line manager is responsible for doing IT security planning and preparing an IT Security Plan. Typically, line managers will complete a separate IT Security Plan for each system under their authority.

4.2.4. IT Security Planning Process

Security planning is an ongoing and continual process. It should be done for new systems as part of design, development, and implementation. As systems mature, security planning should be done to ensure that security risks are managed appropriately as software, hardware, and related conditions change.

4.2.5. IT Security Planning Tasks

IT security planning consists of the following sequence of tasks:

a. Determine the scope.

b. Identify the responsible official and staff.

c. Identify the need for "special management attention."

d. Determine the information category. (See paragraph 4.2.9 for definitions of the categories.)

e. Conduct a risk assessment.

f. Conduct a risk-reduction analysis.

g. Document and justify risks not eliminated.

h. Sign risk summary.

i. Write the IT Security Plan.

j. Obtain authorization to process.

k. Review and update the IT Security Plan.

4.2.6. Determine the Scope

Determining the scope sets the boundaries and areas of focus for IT security planning. Complete the following steps to determine the scope of a system or application:

a. Write a clear statement of the system's functions and describe its operational concept.

b. Identify the intended user community (number of expected users or customers) and any required interfaces with other systems or applications.

c. List the IT resources used in the system (hardware, software, or application).

d. Determine the boundary. Where to draw the boundary line is a matter of choice and logic. However, the following guidelines should help:

(1) Minimize documentation by setting boundaries as broadly as is reasonable.

(2) The boundary determines the line manager's area of responsibility. However, there is some responsibility for security outside of the boundary because of the interconnectivity of IT resources. An acceptable risk for one line manager could be unacceptable to another line manager whose systems are connected.

(3) All IT resources within the boundary become part of one risk management process, which results in one IT Security Plan.

(4) Managers should work together to determine boundaries and ensure that all IT resources are covered in only one IT Security Plan.

(5) The boundary may include one computer or a laboratory full of computers. It may be drawn to include resources that support a common function and category of information. (See 4.2.9 for the categories of information.)

(6) If the system is a large computer network (e.g., LAN or WAN), then firewalls, proxy servers, routers, gateways, cables, and other network components should be considered part of the system.

4.2.7 Identify the Responsible Official and Staff

The line manager assigns a System Administrator for each system. The System Administrator is the "hands-on" security authority for performing the day-to-day security work.

4.2.8. Identify the Need for "Special Management Attention" (Oversight)

Certain systems and software applications, because of the nature of the information in them or the functions they support, require special management oversight and attention. The Center CIO, Center IT Security Manager, Organization Computer Security Officials, and line managers are expected to exercise management judgment in determining which of their systems and software applications require "special management attention." Systems designated to be given "special management attention" need to have their security concerns documented and justified in an IT Security Plan. The Organization Computer Security Official and the CIO shall conduct periodic independent reviews and audits of security controls until special management concerns have been alleviated. The following list describes some specific systems that will require "special management attention."

a. Major Applications--Use of information and IT to satisfy a specific set of user requirements that require special management attention to security. This attention is required due to the risk and magnitude of harm that would result from the loss, misuse, or unauthorized access to or modification of the information in the application.

b. Major Information Systems--Systems that have been designated by the CIO as "major information systems" for OMB A-11 reporting.

c. Mission Critical Systems--Systems that provide Agencywide support, such as wide area networks, Agencywide business functions, command and control of space systems, Agencywide consolidated IT resources, or IT resources that affect life support.

d. NASA Resource Protection (NRP) Facility--IT resources critical to a facility or operation designated under the NRP program by the cognizant program office (ref. NPD 1600.2, NASA Security Program).

e. Center Designated Systems--Other IT systems designated by the Center Director or CIO.

4.2.9. Determine the Information Category

All information stored, processed, or transmitted by NASA's information systems is sensitive to some degree and is entitled to some degree of protection. Various categories of information should be protected using different means, stringency levels, and controls according to the risk and impact of their being altered, destroyed, made unavailable, or disclosed. NASA's experience has been that the information used in conducting the Agency's daily business falls into five categories. These information categories determine the baseline requirements for IT security. (See appendix A for these baseline requirements.) Once managers know the categories and baseline requirements with which they should be concerned, the process of setting controls is considerably simplified. (See Figure 4-2.) The following are the five information categories:

a. Mission (MSN) Information--If the information, software applications, or computer systems in this category are altered, destroyed, or unavailable, the impact on NASA could be catastrophic. The result could be the loss of major or unique assets, a threat to human life, or prevention of NASA from preparing or training for a critical Agency mission. Examples in this category are those that control or directly support one of the following:

(1) Human space flight.

(2) Wide Area Networks.

(3) Development of the data or software used to control human flight.

(4) Training simulation vehicles.

(5) Wind tunnel operations.

(6) Launch operations.

(7) Space vehicle operations.

b. Business and Restricted Technology (BRT) Information--This category consists of information that NASA is required by law to protect. It includes information, software applications, or computer systems that support the Agency's business and technological needs. In general, if information in this category should be disclosed inappropriately, the disclosure could result in damage to our employees, in loss of business for our partners and customer businesses, in contract protest, or the illegal export of technology. This category includes systems containing technological information that is restricted from general public disclosure because of public laws. Examples in this category are those that are related to the following kinds of information:

(1) Financial.

(2) Legal.

(3) Payroll.

(4) Personnel.

(5) Procurement.

(6) Source selection.

(7) Proprietary information entrusted to the Government.

(8) Export controlled technical information (includes disclosure to foreign nationals).

c. Scientific, Engineering, and Research (SER) Information--All official NASA information held by NASA employees may be released publicly only in accordance with NASA regulations; however, systems in this category do not contain information for which the release is otherwise governed by law. This category consists of information that supports basic research, engineering, and technology development but is less restricted against public disclosure.

(1) Alteration, destruction, unauthorized disclosure, or unavailability of the systems, application, or information would have an adverse or severe impact on individual projects, scientists, or engineers; however, recovery would not impede the Agency in accomplishing a primary mission.

(2) Integrity is the driving concern in this category followed by availability. Confidentiality is important and should be considered in a risk assessment insofar as it protects individual researchers from such things as premature disclosure of their work by another party. The impact, however, is primarily on an individual rather than on the Agency.

d. Administrative (ADM) Information--Administrative Information includes, but is not limited to electronic correspondence, briefing information, project/program status, infrastructure design details, predecisional notes, vulnerability descriptions, passwords, and internet protocol addresses. Organizations run various applications-from problem reports to configuration management tools-on administrative IT systems.

(1) This category includes systems, applications, and information that support NASA's daily activities, such as electronic mail, forms processing, networking, and management reporting.

(2) Integrity and availability are the driving IT security concerns. The impact is primarily managerial in nature, which would require time and resources to correct. Confidentiality may be of concern in certain specific administrative information. In such instances, additional security controls must be imposed as a risk analysis dictates.

e. Public Access (PUB) Information--This category includes information, software applications, and computer systems specifically intended for public use or disclosure, such as a public web site or hands-on demonstrations. The loss, alteration, or unavailability of information in this category would have little direct impact on NASA's missions but might expose the Agency to embarrassment, loss of credibility, or public ridicule.

(1) Information posted for public access which could expose NASA missions to risk if compromised should be afforded additional protective measures. In these cases, the baseline requirements for ADM information should be implemented. (For example, contractors may submit proposals based on information from NASA web sites. Loss, alteration, or unavailability of data at the site could result in protests, thereby impacting procurement cycle time and ultimately NASA missions.)

(2) Integrity and availability are the driving concerns. IT security controls are selected to protect the resources themselves and are not intended to protect the confidentiality of the information.

There is no restriction against mixing different categories of information in the same system.
When this occurs, however, the line manager responsible for the operation of the system must
ensure that the proper degree of protection is applied to all information, as determined by the
risk assessment.

Figure 4-2

4.2.10. Conduct a Risk Assessment

The boundaries of the system have now been identified, the need for "special management attention" has been determined, and information has been categorized as to its criticality in the Agency's mission. This information is used as input for conducting the risk assessment process.

a. The risk assessment is a structured process that enables the line manager to do the following:

(1) Determine the risks associated with a system.

(2) Decide how probable it is that the risks will be realized.

(3) Assess the impact of risks if realized.

(4) Rank them in order of seriousness.

(5) Decide which, if any, risks to accept.

b. Line managers often assign analysts (or teams of analysts) to perform risk assessments on their behalf. Upon completion of the risk assessment, the analyst reports the findings and recommendations to the line manager.

c. Whether a system is identified as requiring "special management attention" has no bearing on the process used to assess risk. However, the number of potential risks considered, the depth of the risk analysis, and the number and stringency of security controls may be different, depending on the level of risk that management is willing to accept.

4.2.10.1. Identify the Assets at Risk

The assets at risk are those found within the boundary established in paragraph 4.2.6. The hardware, software, networks, facilities, and information are among the assets to be considered. Storing, transmitting, or processing certain kinds of information often brings with it special restrictions. If, for example, the processing, storage, or release of the information is covered by statute (e.g., Privacy Act, Export Control), the analyst should take special care from the outset.

4.2.10.2. Determine the Nature and Value of the Resources

Information may be the primary asset at risk and more valuable than the systems and software that process it. Therefore, it is imperative that the nature of the information and its value to the organization be known at the outset. The nature of some information, such as personal information, proprietary data, trade secrets, and procurement data, require protection even if it is difficult to place a dollar figure on its value. Knowing the costs associated with replacing or reconstructing IT resources is important in conducting a risk assessment. The following are guidelines for determining the value of different resources:

a. Hardware and facilities--the cost of replacing the functionality of these assets.

b. Software applications--an estimate of the cost to rewrite the software or the cost to replace the software.

c. Information--an estimate of the cost to retrieve or reconstruct the information. Since the value of some information may decrease significantly over time, it is important to factor the time criticality of information into the estimate. For some information, the cost of losing time-critical information may be too high to accept any risk.

4.2.10.3. Identify Threats to the Assets at Risk

Threats are any events or circumstances, whether internal or external, that have the potential to cause harm to a system or to its associated applications or information. A threat could result in the destruction or modification of the computer systems, networks, software applications, or information; the unauthorized disclosure of information; or the denial of the service that the assets are intended to provide. The analyst conducting the risk assessment should list all known threats without regard to their probability of occurrence. The risk assessment should not proceed until the analyst conducting the assessment is satisfied that a comprehensive list of potential threats has been obtained. Make the list of threats as inclusive as possible by doing the following:

a. Contact the Center IT Security Manager's Office for current information on intruder attacks.

b. Review bulletins regarding security weaknesses of equipment, operating systems, and technologies that are incorporated in this particular system or application.

c. Review threats identified by other risk assessments for similar systems at the same location.

d. Review vendor publications or ask the vendor for effective methods of providing security for that vendor's products.

e. Identify single points of failure in the functional design.

4.2.10.4. Identify Vulnerabilities

This step is to determine whether the system is vulnerable to the threats identified in the previous step and in what ways it is vulnerable. A vulnerability is a weakness that can be exploited to violate security processes or controls. If a system or application is vulnerable to a threat, it is considered a risk. (See Figure 4-3.) The relationship among threats, risks, and vulnerabilities is important. A risk is nothing more than a threat to which the system is vulnerable. If there is no vulnerability, regardless of the seriousness of the threat, there is no risk. If there is no threat, regardless of the seriousness of the vulnerability, there is no risk. Managers should not spend scarce resources protecting systems in areas where there is no threat, nor should managers provide further protection against threats to which they are not vulnerable. They do need to be very sure of their decisions. Vulnerabilities are the focus of risk management. Requirements for the risk analyst are as follows:

a. Determine the vulnerabilities--the risk analyst assigned to determine the vulnerability to threats should understand the following:

(1) System's technologies.

(2) Purpose for which the system has been created.

(3) System's user community.

(4) Boundaries.

(5) Baseline requirements (See appendix A for details.)

b. Match vulnerabilities with threats--the analyst looks at each threat and considers it in light of each component that was judged to have value (see 4.2.10.2). The analyst should ask the following questions:

(1) Is the system vulnerable to this threat?

(2) If the system is vulnerable to this threat, what are the vulnerabilities?

c. Assessing vulnerabilities--the analyst assesses each of the threats and considers how the threat might be realized for each of the system's components (or groups of components). While there is no replacement for system knowledge and experience in performing a risk analysis, the following sources provide information on potential vulnerabilities:

(1) Independent audit reports that have been conducted on the system or upon similar systems.

(2) Previous audits of the NASA OIG on the system or on similar systems.

(3) Interviews with system management and development, operations, and maintenance personnel.

(4) Results of penetration tests conducted on the system or on similar systems.

(5) Information from vendors regarding corrected or uncorrected vulnerabilities of that vendor's systems or software.

(6) Bulletins or other archives of information regarding vulnerabilities of various systems.

(7) Experience of individuals who have assessed risk on similar systems.

d. Describe the vulnerabilities--the analyst lists and describes each vulnerability. For example, if the component is a server containing Privacy Act data, one of the threats might be physical access to the equipment. The vulnerabilities might include the following:

(1) The system design calls for the server to be placed in an open office area.

(2) The area proposed for the location of the server is not locked, but it is typically staffed 24 hours per day.

(3) The server will contain information restricted from unlimited public disclosure, but the area is open to visitors who are escorted at all times.

e. Document vulnerabilities--Analysts must document vulnerabilities precisely so that these vulnerabilities can be addressed in further analysis. For example, "Users frequently write cipher lock combination on the door" is a useful statement of a vulnerability, while "Physical controls weak" is not.

> **When identifying vulnerabilities, analysts should consider any other systems to which the system in question is connected. Since systems are normally interconnected, it is possible that the access provided by another system on the network could result in a vulnerability. The analyst should understand any security weaknesses posed by other systems that share common resources.**

Figure 4-3

4.2.10.5. Determine and Prioritize Risks

The analyst has a thorough list of the threats to the system and the system's vulnerabilities to each threat. This step will result in a prioritized list of risks that may be presented to the responsible line manager. The analyst will calculate a risk value for each risk to prioritize the list. There are many methods for calculating the risk value, some of which are objective. They produce quantitative results that must be carefully calculated and documented. Other methods are subjective and require that the analyst document the assumptions made and the process used.

a. The objective approach is based on the notion that a risk value can be determined from a threat probability multiplied by the potential loss resulting from a vulnerability. This approach requires assigning a numerical value to each threat and assigning a probability value to each vulnerability. Some methods for implementing an objective approach can be complex and time-consuming. However, it is possible to develop and use a fairly simple objective process that produces comparable results at far less cost and trouble. (The objective approach is also known as the quantitative method.)

b. The subjective approach is based on the analyst's experience and judgment. This approach usually assigns subjective values, such as "high," "medium," and "low," to each threat and vulnerability. A matrix can be developed that identifies the "high" and "low risks". The "medium" is left to the subjective judgment of the analyst.

c. The analyst adopts any logical and consistent method for determining the risk. Regardless of the method used, management should understand the approach used to determine the risk value, the potential impacts, and the liabilities that may result from their decisions.

4.2.10.6. Identify Available Controls and Processes

The list of prioritized risks identified in the previous step is the basis for selecting the security controls and processes for the system. The analyst will do the following:

a. List the baseline requirements for the information category the system processes or handles (see paragraph 4.2.9). Baseline requirements are derived from "best practices" used by industry and Government and have been targeted to the particular security needs of the information.

b. Study the proposed system and its interfaces to determine what security controls are available. Vendors sell their equipment with a suite of available security controls. The facility into which the system will be placed may afford additional physical controls (e.g., access control for the building and a lockable room in which to install components such as servers). The network to which the system is attached may afford yet other security controls (e.g., a firewall).

c. Review the most current set of recommended controls, tools, and techniques. These can be found in the "NASA IT Security Architecture" document. (Ask your Center IT Security Manager for the most current copy.)

d. List each available control opposite the risk that it reduces or corrects. If the available control is only a partial solution, the analyst should note this on the list.

4.2.10.7. Identify Uncorrected Risks

The analyst's list will show risks that are corrected or at least mitigated by controls provided by the IT equipment. If the available controls correct all the risks, the job is completed, and the analyst prepares the IT Security Plan. However, the analyst may find that there are still substantial risks left uncorrected, and that a number of risks have been mitigated but still require more work for appropriate correction. The risk assessment is concluded at this point. Deciding what to do with the uncorrected risks is the subject of the risk-reduction analysis.

4.2.11. Conduct a Risk-Reduction Analysis

The risk assessment was prepared so that the responsible line manager has an understanding of the threats to the system, vulnerabilities of the system, and a prioritized order of the risks. The line manager may choose either of the following:

a. Do nothing other than to implement the controls that the analyst has recommended and accept the prioritized list of risks. However, the risk assessment may reveal some unacceptable risks, some of which may prompt design or equipment changes. Therefore, it is important to conduct the risk assessment as early as possible in the design of a new project because it reduces the cost of redesigning. (The life-cycle process described in section 4.1 recommended that risk assessment activities begin in the project initiation phase and be essentially completed by the project definition phase.)

b. Have the analyst use the results of the risk assessment to provide recommendations on the risks that have not been addressed and risks that have been partially addressed.

4.2.11.1. Identify Potential Controls for Remaining Risks

For each uncorrected risk, the analyst recommends a security control that will either correct the risk or at least mitigate it to the extent possible. There are three types of controls as follows:

a. Technical controls--those provided by the manufacturer of the system or software application as well as third party products. Generally, these controls are inherent in the operating system or application (e.g., the ability to restrict account access or the ability to force password changes at predetermined intervals). These controls are recommended as the first line of defense.

b. Physical controls--those provided by the facility in which the system runs (e.g., a cipher lock for controlling admittance to the facility or access to fire suppression equipment).

c. Procedural controls--those invoked as a result of actions that system personnel take (e.g., required procedures for documenting configuration changes, using sign-in logs, and completing forms or checklists). These controls tend to be the weakest and require management enforcement and continuing training to be effective.

4.2.11.2. Determine Feasibility of Recommended Controls

At this point, the analyst considers each of the recommended controls and determines its operational feasibility. Some controls are feasible, but implementing them would significantly reduce the ability of the system to function at an acceptable level. Some may be implementable, but the life-cycle cost would be excessive. There is usually more than one way to solve an IT security problem. The analyst's responsibility is to provide cost-effective controls that mitigate, if not fully correct, each of the risks.

a. In determining the operational feasibility, the analyst should consider the following:

(1) The system or software application vendor may have already provided a technical control, which might be a matter of invoking an existing option in the operating system or application software. Invoking these controls often results in a cost, usually paid in terms of processing overhead or a reduction in ease of use. The analyst must weigh the benefits gained against the costs.

(2) Physical and procedural controls may be used to supplement or substitute for technical controls. Although it is tempting to view procedural and physical solutions as being "free" since they can often be implemented with existing resources, effectiveness, as well as training, administration, and enforcement costs must be considered.

(3) The physical control of IT resources is extremely important and must be considered in addition to technical and procedural controls.

b. Each security control has a cost that the analyst must consider before deciding on a recommendation. All three kinds of controls must be balanced to arrive at a comprehensive, cost-effective solution. Costs are paid in various ways. Some costs are paid in dollars, some are reflected in system overhead, and some appear as user inconvenience. The analyst must determine a cost-effective control to mitigate or correct each risk. If no control can be found, then the risk reduction analysis must state this fact.

c. The analyst may also find security controls available that have no risks or baseline requirements associated with them. If they are expensive to implement, it is appropriate to document and justify why these controls are not being implemented or indicate why they are not applicable.

d. Before concluding the risk reduction analysis, the analyst must consider any security controls that should be imposed to mitigate risks to those who share common resources. These controls and their costs must be included in the presentation to management.

e. To document the risk reduction analysis, the analyst will annotate the prioritized list of risks with recommended controls for each risk and the cost of implementing each control. The analyst is ready to present the results of the risk reduction analysis to management.

4.2.11.3. Decide on an Acceptable Level of Risk

Upon completion of the risk reduction analysis, the analyst will present the recommendations to line managers who are responsible for determining acceptable levels of risk. Because line managers are ultimately responsible, they may accept the recommendations as given by the analyst or reprioritize them as necessary. Sometimes a line manager may be faced with either accepting a high risk or not processing. It is not the intent of the NASA IT Security Program to prohibit processing in high-risk situations. The line manager must do the following:

a. Seek Senior Management and/or legal advice for systems requiring "special management attention" and where the laws or policies apply to the risk decision.

b. Decide which recommendations to implement and which risks to accept, based on the realities of budgets, schedules, and deadlines.

c. Ensure that, in accepting risks, line managers understand the consequences. Line managers are within their rights to grant an authorization to process, provided the IT Security Manager agrees that other Center systems are not put at risk. When line managers and the IT Security Manager cannot reach agreement, the Center CIO and Center Director will make a determination.

4.2.11.4. Document and Justify Risks Not Eliminated

The line manager writes a risk summary, which documents each of the remaining risks, and notes the reason these risks are not being addressed. This documentation will provide the rationale for the line manager's decisions to accept certain risks. The line manager will also use this information to prepare the IT Security Plan.

4.2.11.5. Apply Controls

This step puts the selected security controls in place. All risk-reduction activities must have appropriate implementation schedules, personnel assignments, testing, training, documentation, and budgets. If the system is large and complex or if the system is designated as requiring "special management attention," a separate plan may be appropriate.

4.2.12. Write IT Security Plan

The IT Security Plan is the culmination of the work done during the IT security planning process. (Paragraph 5.1.2. describes the content and organization of this plan.) The plan is the source document that describes how the security controls for a particular system function. Documentation from the risk analysis, risk reduction analysis, and management decisions is used to prepare the IT Security Plan. This contributing documentation may be subject to review and audit by external agencies and should be retained with the plan and modified when significant changes occur.

4.2.12.1. Authorizing the System to Process

A cover letter or an approval sheet should be attached to the IT Security Plan with the signatures of the responsible line manager and any affected data owners. This cover letter or approval sheet is the document that authorizes the system to process. When a new data owner is to process data on the system, the new data owner needs to sign the IT Security Plan as concurring on the acceptability of the system to protect their data.

4.2.12.2. Protecting the IT Security Plan

An IT Security Plan is a sensitive document, as it may discuss uncorrected vulnerabilities and may mention risks that have been accepted. Document covers and transmittal sheets should be used as appropriate. These plans should be distributed only on a need-to-know basis. The line manager should submit the IT Security Plan to the Organization CSO.

4.2.13. Review and Update the IT Security Plan

4.2.13.1. The IT Security Plan, described in the previous paragraph, discusses the security status of a system at a particular point. As conditions change, it is important that the line manager periodically review the system's security and update the plan as necessary.

4.2.13.2. Reviewing a system's IT Security Plan is one of the line manager's responsibilities. Reviews for these plans are required at least every 3 years or upon significant change, whichever comes first. If the system has changed so much that the current IT Security Plan no longer describes the category of information, system or application, the line manager must update the plan, reissue it, and re-authorize the system to process.

4.3. IT Security Awareness and Training

4.3.1. Overview

4.3.1.1. NASA is responsible for providing its civil service and contractor employees with training in IT security concepts, policies, and practices. The Computer Security Act of 1987, Pub. L 100-235 and OMB A-130, Appendix III mandate periodic training in IT security awareness and accepted IT security practices for all employees using, managing, or designing systems. Also, mandatory training must be completed before an employee is granted access to systems.

4.3.1.2. To meet this requirement, NASA has adopted the "learning objectives" approach developed by the National Institute of Standards and Technology (NIST). This approach prescribes that IT security training provide employees with the IT security knowledge required for them to do their jobs. The paragraphs that follow provide guidelines for determining the IT security training needs of employees who design, program, operate, or use NASA's computer systems.

4.3.1.3. To the extent possible, the training outlined in this chapter should be incorporated into existing NASA training programs rather than as a separate training program.

4.3.2. Training Approach

A method is needed to ensure that appropriate IT security awareness and training is provided to each employee. By identifying the audience category and the subject matter for the training, it is possible to create a matrix that assigns a training level to this combination of audience category and subject matter. (See paragraph 4.3.6 for this matrix.) The approach for determining appropriate training for employees relies on the following factors:

a. Audience category.

b. Subject matter areas.

c. Training levels and goals.

4.3.3. Audience Categories

For the purpose of providing training relevant to employees' needs, employees involved in the management, design, operation, and use of computer systems are divided into the following six audience categories:

a. Executives are Senior Managers who are responsible for setting Agency and Center IT security policy, assigning responsibility for implementing the policy, determining acceptable levels of risk, and providing the resources and support for the IT Security Program.

b. Program and Functional Managers are managers and supervisors who have a program or functional responsibility (not in the area of IT security) with the Agency. They have primary responsibility for the security of their data and/or systems. This means that they designate the information category of the system, assess the risks to the systems and information, and identify the security requirements to the supporting data processing organizations, CCS staff, IT Security Manager staff, and users of their data. Functional managers are responsible for ensuring the adequacy of all contingency plans related to the safety and continuing availability of their data.

c. IRM, Security, Procurement, and Audit Personnel are involved with the daily management of the Agency's information resources, including the accuracy, availability, and safety of these resources. These individuals typically issue procedures, guidelines, and standards to implement the Agency's and Center's policy for IT security, and to monitor its effectiveness and efficiency. They provide technical assistance to users, functional managers, and the data processing organization in such areas as risk assessment, threat assessment, vulnerability analysis, and security product and technology availability. They review and analyze functional and program groups' performance in IT security. They ensure that security requirements are built into the procurement of information systems and that requirements for the personnel screening and training of support contractors are addressed in the SOW.

d. Office of Procurement and staff are responsible for acquiring IT resources and services. They should ensure that acquisitions include appropriate security requirements for IT security plans, tools, and controls and for complying with NASA policies, regulations, and procedures. They should also ensure that specific IT security requirements are addressed in SOW and "Request for Proposals" (RFP).

e. IT Resource Management, Operations, and Programming staff are involved with the daily management and operations of the IT services. They protect the data in their custody and identify to data owners the security measures used to protect these data. This group includes such diverse positions as computer operators, System Administrators, database administrators, systems and applications programmers, postmasters, webmasters, network engineers, network security administrators, systems analysts, computer specialists, and telecommunications specialists. They provide the technical expertise for implementing security-related controls within the IT environment. They have primary responsibility for all aspects of contingency planning.

f. End Users are employees who have access to NASA computer systems and networks that process, store, or transmit information. This is the largest and most heterogeneous group of employees. It consists of everyone, from an executive with a desktop system to application programmers to data entry clerks.

4.3.4. Subject Matter Areas

NASA is adopting NIST's approach, which identifies the following six subject matter areas:

a. IT Security Basics is an introduction to the basic concepts behind IT security practices and the importance of protecting information from vulnerabilities to known threats. This basic training also addresses computer ethics.

b. Security Planning and Management is concerned with risk analysis and penetration testing, the determination of security requirements, security training, and the internal Agency organization that is responsible for IT security.

c. IT Security Policies and Procedures examines Governmentwide and Agency-specific security practices in the following areas of security: physical, personnel, software, communications, data, information, industrial, and administrative.

d. Contingency Planning covers concepts relevant to all aspects of contingency planning, including emergency preparedness planning, backup plans, disaster recovery planning, continuity of operations planning, and recovery plans. It identifies the roles and responsibilities of all parties involved.

e. Systems Life-Cycle Management discusses how security is addressed during each phase of a system's life cycle. It addresses procurement, certification, and accreditation of systems and their related environments.

f. Advanced System Security covers the skills needed to install preventive security controls, analyze log data for intrusion detection, assess risks and vulnerabilities, establish "rules of the system," conduct self-evaluations, evaluate the impacts resulting from implementing security controls, plan risk-reduction activities, and conduct testing of contingency plans.

4.3.5. Training Levels and Goals

The level of training required in each subject matter area will vary across NASA from general awareness training to specific courses as determined by NASA. Not every training level is needed for a given audience category or a given content area. The levels of training and their goals are as follows:

a. Awareness training is expected to create a sensitivity to threats and vulnerabilities and the need to protect data, information, and the means of processing data and information.

b. Policy training provides the ability to understand IT security principles so that informed policy decisions about computer and information security programs can be made.

c. Implementation training provides the ability to recognize and assess the threats and vulnerabilities to IT so that managers can set security requirements that fulfill NASA policies, procedures, and guidance.

d. Performance training provides employees with the skills to design, execute, and evaluate Agency IT security policies, procedures, and guidance. The objective of this training is to enable NASA employees to apply security concepts while performing the tasks that relate to their particular positions. This level of training may require education in basic principles and state-of-the-art technology.

4.3.6. Training Matrix

Using the audience categories, subject matter areas, and training levels and goals described in the preceding paragraphs, it is possible to portray NASA's IT security awareness and training approach in a matrix. The matrix shown in Figure 4-4 depicts NASA's concept of who should be trained and the level of performance that is to be achieved by each audience.

4.4. IT Security Incidents Reporting and Handling

4.4.1. Overview

Despite all the best efforts that an organization can expend, an IT security incident sometimes occurs. When an incident occurs, the NASA community has an incident response process in place to assist the affected organization in responding to the event and returning as quickly as possible to normal operations.

4.4.2. IT Security Incident

4.4.2.1. An IT security incident is an adverse event or situation associated with a system that poses a threat to the integrity, availability, or confidentiality of data or the systems and that results in (i) a failure of security controls; (ii) an attempted, suspected, or actual compromise of information; or (iii) the waste, fraud, abuse, loss, or damage of Government property or information.

4.4.2.2. An IT security incident may often be recognized by its outcome-an unauthorized person possesses information or technology, information may be wrongly disclosed, information or systems may be altered in an unauthorized manner, or information or systems may not be accessible when needed. In some cases, these events may involve violations of Federal or State law.

	IT Security Basics	Security Planning and Mgmt	IT Security Policies and Procedures	Contingency Planning	System Life Cycle Mgmt	Advanced Systems Security
Executives	A	PO	A	A	A	A
Program and Functional Managers	A	I	I	PF	PF	A
IRM, Security, Procurement and Audit Personnel	A	PF	PF	PF	PF	PO
IT Resource Mgmt, Operations, and Programming Staff	A	PF	PF	PF	A	PF
End Users	A	A	PF	PF	A	A

LEGEND
A= Awareness PO= Policy I = Implementation PF = Performance

Figure 4-4

4.4.3. Responsibility for Reporting IT Security Incidents

Everyone who uses NASA IT resources is responsible for reporting any known or suspected IT security incidents. (See paragraph 4.4.7.) Employees must notify their System Administrator, CSO, or Center IT Security Manager and not widely disseminate the information.

Employees who discover an IT security incident are victims, not criminals.

Figure 4-5

4.4.4. Responsibility for Handling IT Security Incidents

The Center IT Security Manager bears primary responsibility for responding to IT security incidents and ensuring that they are handled according to the guidelines in this section. The Center IT Security Manager has the responsibility for reporting incidents to Center management, for reporting incident metrics to the PCITS, and for reporting incidents, as noted below, to the NASA Automated Systems Incident Response Capability (NASIRC) to facilitate Agencywide and interagency coordination and handling of incidents affecting Government systems.

4.4.4.1. The Center IT Security Manager will report all incidents to NASIRC except for the misuse of IT resources and for previously known viruses unless the virus caused a major impact and might affect other Centers.

4.4.4.2. The Center IT Security Manager usually will call upon other staff or form a team to respond to incidents.

4.4.5. Priorities for Handling IT Security Incidents

The NASA CIO has established priorities, which the Center IT Security Manager will honor in handling all incidents. These priorities are as follows:

a. Protect Government IT resources and information and help the affected system to return to normal operations as soon as feasible.

b. Collect information to support criminal, disciplinary, or other appropriate actions against perpetrators.

4.4.6. How to Recognize an IT Security Incident

It is not always possible to look at an affected computer and tell what occurred. Without analysis, computer crimes, maintenance problems, and operator errors often look alike. If in doubt, contact your System Administrator for assistance. Some of the more common symptoms of incidents follow.

4.4.6.1. Security Incidents Related to Computer Files

a. Files that should be accessible to a user are suddenly unavailable.

b. Files have been edited, though no changes in them should have occurred.

c. Files appear, disappear, or undergo significant and unexpected changes in size.

4.4.6.2. Security Incidents Related to User Accounts

a. User accounts appear or disappear from the system without the knowledge or consent of the System Administrator.

b. A user's password has been changed without the user's knowledge or involvement.

c. An employee's account suddenly becomes active, but the employee is not present to use it and the employee is known not to be using it remotely.

d. System logs record numerous unsuccessful logon attempts to a given user's account, but the user is not the one who attempted the logons.

e. Parts or all of the system logs are missing, or logs appear altered.

f. System logs indicate successful logons to a user's account but are at odd hours for that user.

4.4.6.3. Security Incidents Related to Application Software

Application software has been modified, but changes have not been approved.

4.4.6.4. Security Incidents Related to Physical Areas

a. Output of a sensitive nature that would normally be handled carefully is found in printer trays or left uncontrolled in the work area.

b. Unauthorized personnel are discovered in the work area.

4.4.6.5. Security Incidents Related to Viruses

a. Files that should be accessible to a user are suddenly unavailable.

b. Files have been edited, though no changes in them should have occurred.

c. Files appear, disappear, or undergo significant and unexpected changes in size.

d. The system displays strange messages or mislabels files and directories.

e. The system becomes inaccessible, (e.g., it will not boot properly)

f. Data on the system hard drive is no longer accessible.

4.4.7. Reporting IT Security Incidents

For IT security incidents, members of the NASA community should proceed as follows if they have discovered or think they have discovered a security incident:

a. Immediately notify the System Administrator, line manager, Organization Computer Security Official, or Center IT Security Manager per Center guidelines and await assistance. Do not try to track or catch an intruder as such attempts may alert the intruder, who could destroy evidence.

b. Leave the equipment alone. Do not try to process, insert, or delete any information on the affected equipment.

c. If a virus begins to execute and it appears that the virus is damaging files on the workstation, immediately shut down the workstation by turning off the power and call for assistance.

4.4.8. Handling Incident Information

Upon receiving notification of an IT security incident or a suspected incident, the Center IT Security Manager will immediately dispatch a team or staff member to obtain more information. Any member of the NASA community who has questions about discussing or releasing IT security incident information must consult with their Center IT Security Manager.

4.4.8.1. Handling Incident Information/ Response Team

The team will interview all individuals who have information about the incident. The team will also ask for access to any or all of the following:

a. Two disk "image" backups of the disk or disks on the system (e.g., those created using the "dd" Unix command).

b. Any applicable audit trails or system logs.

c. Any exception reports (i.e., summaries of security-relevant events extracted from more extensive system logs).

d. Any available system monitoring reports.

e. An account with system privileges to examine the system.

f. Any available documentation that will help the investigator understand the affected system and its connectivity.

4.4.8.2. Handling Incident Information/ Center IT Security Manager

The Center IT Security Manager will prepare an incident report and normally will be the only official to release this information outside the Center. The Center IT Security Manager will establish a procedure for reviewing and getting concurrence on incident reports with the Center CIO. In certain cases, the Center IT Security Manager's incident reports may also be reviewed by the Center Director, Human Resources Office, Office of Chief Counsel, and Office of Public Affairs before being released.

4.4.8.3. Handling Incident Information/ Sharing Data

Individuals with knowledge of an incident must exercise caution to keep information within prescribed channels. Failure to do so may impede or even preclude the Government's chance of obtaining a conviction if a crime is discovered, or it may cause needless embarrassment to others if what appears at first to be a crime later proves not to be. All electronic communications regarding incidents will be conducted in a secure manner through the use of secure messaging technology. Examples of personnel authorized to possess incident information include the individual's System Administrator, management chain, corporate security officer (if applicable), Organization Computer Security Official, Center IT Security Manager, local Office of the Inspector General, CIO, and Center Director. Other officials from the CCS Office, Human Relations Office, and Office of Chief Counsel may become involved if the situation warrants it.

4.4.9 Procedures Related to Computer Crimes

4.4.9.1 The Center IT Security Manager will perform an initial analysis to determine if an incident has occurred and whether the incident is a computer crime. Since time is of the essence in recognizing and thwarting threats to the Agency's IT systems and in collecting evidence needed for possible prosecution of computer crimes, the initial analysis should be rapid. Incidents that may constitute a computer crime include the following:

a. Compromise of system privileges (root access).

b. Compromise of information protected by law (e.g., International Traffic in Arms Regulations, Privacy Act data, procurement sensitive data).

c. Denial of service of major IT resources.

d. Child pornography.

e. Malicious destruction or modification of NASA data and/or information.

4.4.9.2 The Center IT Security Manager, in conjunction with Center management, should be vigilant as to other categories of incidents, such as unauthorized disclosure of sensitive technology/program data, unauthorized user access, and probes and scans which are clearly discernible as having hostile intentions. When in doubt about the possible criminality of these incidents, the Center IT Security Manager should consult with the local OIG or Headquarters Computer Crime Division.

4.4.9.3 Incidents confirmed by initial analyses to be compromises of system privileges (root access) or denial of service of major IT resources must be reported immediately to the NASA OIG and to the CCS. Following completion of the initial analysis of other types of incidents, the IT Security Manager will notify Center management, including the CCS, if the initial analysis indicates that the security incident may constitute a computer crime.

4.4.9.4 For incidents, other than root access and denial of service of major IT resources, that initial analysis determines may constitute a computer crime, the CCS, working with the IT Security Manager, may conduct, at the discretion of Center Management, preliminary investigations to determine the nature and magnitude of threats posed by those incidents to the Center. Those incidents, confirmed by Center Management to be computer crimes, will be reported to the NASA OIG as soon as possible, but no more than 24 hours after completion of initial analysis, in order to preserve evidence and to allow the OIG to conduct its investigations without undue delay. If, after 24 hours past completion of initial analysis, it is still unclear whether the incident is a computer crime, the incident will be reported to the OIG as a possible computer crime.

4.4.9.5 During the course of preliminary inquiries into incidents that could possibly involve computer crimes, the CCS and IT Security Manager may contact external groups and other organizations to better understand the threat posed by the incidents, to share information concerning incidents, and to develop recommendations for Center management regarding the best course of action in dealing with incidents. Referrals of computer crimes to the Department of Justice and other external law enforcement organizations will be performed by the OIG.

4.4.9.6 Since handling evidence of a computer crime involves a set of complex rules of evidence, the Center IT Security Manager will consult with the CCS and OIG regarding appropriate evidence handling procedures.

4.4.9.7 The Center IT Security Manager's staff and affected line managers will assist the OIG in investigating, monitoring, and gathering evidence necessary to identify and prosecute individuals committing computer crimes involving NASA assets. However, there may be circumstances, when permitting a security incident to continue in order to provide prosecutorial data, that will leave NASA or its customers open to unacceptable risks. For that reason, the Center Director/Associate Administrator for Headquarters Operations or their designee must do the following:

a. Decide, after coordination with the OIG if feasible, whether to control/terminate incidents when, in their judgment, NASA's missions, its customers, its reputation, or its assets are in jeopardy, or to allow incidents to continue in order to collect information related to possible prosecution of attackers. In doing so, the decision-maker must take into account the value of the assets at risk and their vulnerability to damage or loss.

b. Inform, in a timely fashion, the local OIG and/or other law enforcement groups that may be working on the incident of any actions taken to control/terminate and work with them to minimize the loss of information, consistent with the protection of NASA resources.

c. Whenever possible, provide advance notification to and coordinate with the OIG the orderly control/termination of an incident. If advanced notification and coordination is not possible, reasonable steps should be taken to preserve evidence, notification to the OIG should be made as soon as feasible, and the reason for not providing advanced notification and coordination with the OIG will be documented to the Manager of the Principal Center for IT Security.

4.4.9.8 If the incident involves computer misuse and a computer crime has not occurred, the Center IT Security Manager will complete the analysis and refer the incident to the appropriate Center line management, Human Resources Office, and/or the Office of Inspector General for appropriate action.

4.4.10. Returning Equipment to Service

4.4.10.1. The Center IT Security Manager will return equipment to service as quickly as possible following an incident. In most cases, equipment will be returned to service the same day. The type and scope of each incident will determine the timeframe required to return affected systems to service. The underlying vulnerability that caused the incident to occur must be identified and removed or mitigated prior to returning a system to service. System backups by themselves do nothing to resolve an IT security incident and are done primarily to preserve evidence.

4.4.10.2. Usually, he line manager will use threat information from the Center IT Security Manager, CCS, and OIG to decide whether a system will be removed from service, patched, or remain in service. In some cases, the risk to other systems will mandate that risk-reduction action take precedence over returning the system to operational status. On rare occasions, if the seriousness of an incident warrants it, equipment may be removed from the area and held as evidence.

4.4.11. Categorizing Incidents for Reporting

Defining and tracking categories of incidents provides statistical data that can assist management in allocating resources to improve the IT security posture of the Agency and its Centers. To understand the nature and extent of threats to IT resources, NASA has defined the following seven categories of incidents, based upon severity to the system:

a. System compromise.

b. Information compromise.

c. Unauthorized access.

d. Denial of service.

e. Misuse.

f. Hostile probes.

g. Other IT Security concerns.

4.4.11.1. System Compromise

The following are acts that represent a system compromise:

a. Any account or application that has system privileges is used without prior authorization or approval. (See Figure 4-6.)

b. A weakness in the system is successfully exploited, and access is gained to accounts with system privileges.

c. A valid account is used to increase its own privileges and is successfully exploited to gain access to accounts with system privileges.

Definition of System Privileges

Before discussing the signs of each incident category, it is important to define "system privileges." System privileges are the ability to make modifications to the computer's operating system, system audit logs, system configurations, account privileges, account passwords, data files, software, or applications; to add or delete accounts; to install or delete software and applications; or to alter the system's security controls outside those abilities normally authorized for an individual's account

Figure 4-6

4.4.11.2. Information Compromise

The following are acts that represent an information compromise:

a. A valid account is used without authorization, and access is gained to password files, data, applications, or accounts
that are protected or restricted, but access is not gained to accounts with system privileges.

b. A weakness in the system is successfully exploited and is successfully used to gain access to password files, data, applications, or accounts that are protected or restricted, but access is not gained to accounts with system privileges.

c. The physical theft of assets provides access to password files, protected or restricted data, licensed applications or software, or restricted applications, software, or code.

4.4.11.3. Unauthorized Access

The following are acts that represent unauthorized access:

a. A valid account is used without authorization, but access is not gained to password files, data, applications, or accounts that are protected or restricted outside of the account's authorizations.

b. A weakness in the system is successfully exploited, but access is not gained to data, applications, accounts with system privileges or password files, or accounts that are protected or restricted outside the exploited function's authorization.

4.4.11.4. Denial of Service

The following are acts that represent a denial of service:

a. A system's ability to perform its normal functions is impaired due to its being inundated with activity originating from one or more sources.

b. Resources, such as power, network access, or routing tables, are deliberately modified to cause a system to not be able to perform its normal functions.

c. Malicious code interferes with a system to a significant degree. (Malicious code includes, but is not limited to, viruses, Java applets, ActiveX, trojan horses, logic bombs, worms, unauthorized scripts, daemons, or similar programs.)

d. Assets have been physically taken or destroyed, but no password files, protected or restricted data, applications, restricted software, or code were compromised.

4.4.11.5. Misuse of Information Technology Resources

The following are acts that represent the misuse of IT resources:

a. An authorized account is used in violation of Federal laws, NASA, or Center policies regarding proper use of IT resources.

b. Resources or privileges higher than those allocated or assigned are obtained without authorization.

c. Unlicensed software or applications are installed.

4.4.11.6. Hostile Probe

The following are acts that represent a hostile probe:

a. Exploits are run against a system that would, if successful, have resulted in a system compromise, information compromise, or unauthorized access.

b. Exploits are run against a system that would, if successful, have impaired the system's ability to perform its normal functions.

c. Illicit information gathering or attempted gathering is directed against one or more systems.

4.4.11.7. Other IT Security Concerns

Questionable events that do not fit into the other categories, such as suspicious network activity, excessive junk mailing, chain letters, mail spoofing, or hoaxes that are determined by the Center IT Security Manager to be of concern.

4.5. Personnel Screening

4.5.1. Overview

4.5.1.1. "Public Trust" positions are those which have the potential for action or inaction by their incumbents to affect the integrity, efficiency, or effectiveness of assigned Government activities. The potential for adverse effects includes action or inaction that could diminish public confidence in the integrity, efficiency, or effectiveness of assigned Government activities, whether or not actual damage occurs. (Reference: 5 CFR Part 731)

4.5.1.2. Some positions require special access privileges in order to do the assigned job or duties. These are "Public Trust" positions since they can affect the integrity, efficiency, or effectiveness of the system to which they have been granted privileged access. Screening for suitability, prior to being granted access, is required. This screening is required to ensure that granting any special access privileges to someone would not cause undue risks to the system for which that person has these privileges (e.g., screening would ensure that a convicted embezzler would not be granted access to a payroll system).

4.5.2. Responsibilities and Authority

Line managers are responsible for requesting suitability screening for the staff in their respective organizations, but they do not conduct, contract for, or otherwise participate in personnel security investigations. Only the CCS is authorized to initiate or conduct personnel security investigations.

4.5.3. Determining Who Needs Screening for Privileged Access or Limited Privileged Access

4.5.3.1. All individuals who require privileged access or limited privileged access will require screening. To help define access privileges, this document identifies the following types of access:

a. Privileged access--Can bypass, modify, or disable the technical or operational system security controls.

b. Limited privilege access--Can bypass security controls for part of a system or application but not the entire system or application.

c. Non-privileged access--Cannot bypass any security controls.

4.5.3.2 Appendix A describes baseline requirements related to privileged users and programs.

4.5.4 Security Investigations Process for Privileged Access or Limited Privileged Access to Unclassified Systems

4.5.4.1. The CCS and the Center IT Security Manager will establish a process to identify those needing screening and conduct required investigations. The level of investigation that a user may receive depends upon U. S. law and Federal and Agency policy. Laws and policies regarding personnel investigations change from time to time and should be reviewed with the local Human Resources Office and CCS, in consultation with the Agency or Center legal counsel.

4.5.4.2. See NASA's existing Personnel Reliability Program for Mission Critical Space Systems at 14 CFR 1214.5, for typical personnel screening procedures and criteria that may be applicable to the IT personnel screening process.

4.5.4.3. The security investigation process is as follows:

a. The line manager submits the full name, level of privileges required, and contact information for each individual who requires a security investigation.

b. Using the information provided by the line manager, the CCS staff begins the investigation by contacting the individual and asking for more information. The CCS staff conducts the investigation.

c. The CCS staff will report a favorable or unfavorable result back to the appropriate adjudicating official.

d. Information acquired throughout the screening process shall be protected in a manner consistent with the Privacy Act, and other pertinent laws, regulations, or directives.

4.5.5. Special Considerations for Non-NASA Employees or Contractors

If a user is not a NASA employee or contractor, the following considerations apply for security investigations:

a. Remote users other than NASA employees or contractors--A current Federal investigation performed by the user's parent organization is acceptable if privileged access to a NASA computer system is required. If a remote user requires privileged or limited privilege access and has not been investigated by the user's parent organization, the user's NASA sponsor must request an investigation.

b. International partners--International partners who seek access to U. S. Government IT resources, pursuant to an international agreement, must still be investigated. NASA Headquarters handles all investigations for representatives of foreign governments. Contact your CCS for more information.

4.5.6. Unfavorable Investigation Findings

Sometimes individuals may be denied privileged access as a result of a personnel security investigation. Individuals who are Government employees have the right to contest the findings of these investigations and may do so by contacting the CCS's office; contractor employees need to contact their employer's appropriate point of contact, as the relationship between the Agency and the contractor is governed by the terms and conditions of the contract. For example, in appropriate circumstances, civil service personnel may appeal to the Merit Systems Protection Board in accordance with 5 CFR Part 731.

4.6. Penetration Testing

4.6.1. Overview

4.6.1.1. Despite the best efforts to include security measures and implement security controls in a system or application, there is no guarantee that these measures and controls will reliably prevent security incidents over time. Penetration testing is a way to determine how well security measures and controls work at a particular point in time.

4.6.1.2. While passing penetration tests can demonstrate a level of protection, it is only a snap shot in time. There could be weaknesses that were overlooked (not tested), unknown at the time of testing, and new weakness introduced with new software or system upgrades. Managers should not have a false assurance of security, but be proactive to ensure that system security is maintained.

4.6.1.3. The results of penetration tests are very sensitive and, depending on the system being tested, may even be classified national security information. The test plan should include the measures that will be taken to protect the results of the test. The Center Security Officer should be consulted if the system is one that is known to require "special management attention." Before being released, all deficiencies found in the system must be corrected and retested.

4.6.2. A Penetration Test

A penetration test is an activity in which a test team attempts to circumvent the security processes and controls of a computer system. Posing as either internal or external unauthorized intruders (or both, in different phases of the test), the test team attempts to obtain privileged access, extract information, and demonstrate the ability to manipulate the computer in what would be unauthorized ways if it had happened outside the scope of the test.

4.6.3. Responsibility for Conducting Penetration Tests

Penetration tests may be conducted by either an organization or by the Center IT Security Manager. When an organization conducts a penetration test, the Organization Computer Security Official is responsible for assembling test teams and ensuring that the test is conducted according to the guidelines described in this section.

4.6.4. Types of Penetration Tests

The guidelines that should be followed are related to the type of penetration test being done. The following are the types of penetration tests:

a. Penetration tests conducted by organizations--Any NASA organization may conduct a penetration test of the systems and software applications under that organization's management cognizance. A penetration test conducted by an organization is part of a system's normal life cycle. Organizations may want an independent test and request the Center IT Security Manager or a third party to conduct the testing. (If a third party does the testing, the Center IT Security Manager must be notified).

b. Penetration tests conducted by the Center IT Security Manager--The Center IT Security Manager may conduct an independent test of the security of any system or software application under the Center's cognizance. (See Figure 4-7.) Such penetration tests may be requested by the CIO, Organization CSO's, or the management of the system or software application.

To come under the Center IT Security Manager's purview, the proposed target system must be one in the NASA community in which information is processed by or on behalf of the Federal Government. The Center IT Security Manager will not conduct penetration tests on systems operated by NASA contractors that contain only information belonging to that contractor.

Figure 4-7

4.6.5. Guidelines for Penetration Tests Conducted by Organizations

4.6.5.1. Before an organization conducts its own penetration test, the Organization CSO supervising the test team's activities will do the following:

a. Obtain authorization to conduct the activity from the Center IT Security Manager, either the line manager under whose management cognizance the proposed target system falls or the Center CIO, or designee. (Unless the response of line management is being tested, the line manager under whose management cognizance the proposed target system falls should be notified.)

b. Advise the Center CIO of the circumstances of the test. At a minimum, the Organization CSO will provide the Center CIO with the following information:

(1) Purposes that the test will achieve.

(2) Planned dates and times of the test.

(3) Planned target systems.

(4) Boundaries of the test.

(5) Test methods to be employed.

(6) Names of the civil service personnel who will supervise and be accountable for the activity.

(7) Procedures that will be used in case of an inadvertent violation of the test boundaries.

c. Ensure that no systems that belong to a contractor and that process only information belonging to that contractor will be included in any penetration test.

d. Agree to suspend testing at once if the Center IT Security Manager notifies the test team that NASA is being subjected to an actual intrusion. (Testing may resume as soon as the Center IT Security Manager notifies the test team that the actual situation has been stabilized.)

4.6.5.2. If a test boundary is violated for any reason during the penetration test, testing will cease. The Organization Computer Security Official supervising the test will document the extent of the boundary violation and notify the Center IT Security Manager immediately.

4.6.5.3. Once the penetration test has been completed, the Organization Computer Security Official supervising the test will review the results with the Center IT Security Manager and CIO. Results from the testing will be used to determine if further security enhancements will be required to the system.

4.6.6. Guidelines for Penetration Tests Conducted by the Center IT Security Manager

The Center IT Security Manager uses a structured and carefully controlled process for all penetration testing using the following guidelines:

a. All penetration tests will be coordinated with the organization under whose management cognizance the proposed target system falls. The usual route is through the Organization Computer Security Official.

b. Before penetration testing can begin, a test plan is required. Usually, this test plan will be presented in the form of a briefing to the line manager or Organization Computer Security Official requesting the test. If the Center IT Security Manager initiates the test, the test plan will be presented to the Organization Computer Security Official and to management, as the Organization Computer Security Official requests. It is the organization's choice whether or not to advise their System Administrators and users that a test will take place.

c. Extreme care will be taken by the team to not interfere with operations, alter any system configurations, modify any files, or add any data or information. If any of these restrictions does occur, the affected party will be immediately notified and testing will be stopped.

d. Testing will be scheduled to avoid periods of critical processing for the organization as determined by system management.

e. If a violation of any test boundary occurs, testing will be immediately stopped, the extent of the boundary violation will be documented, and the affected system management will be notified.

f. If an actual intrusion is discovered anywhere in the Center's community while penetration testing is ongoing, testing will be suspended immediately and will remain suspended until the actual situation has been stabilized.

g. The penetration test will conclude with a report to the manager who requested the test. An interim report will be made at any time during the test if a critical vulnerability is discovered.

h. The organization whose systems are targeted under a penetration test will be encouraged to participate in the test activities.

i. The results of any penetration test will be provided upon request to the CIO or to the Center Director through the CIO. Results from the testing will be used to determine if further security enhancements will be required to the system.

4.7. Granting Access

4.7.1. Overview

Line managers have the authority and responsibility for granting access to IT resources under their control. Line managers should think of decisions to grant access as risk decisions, weighing the potential costs and benefits to the Government. Except where specifically limited by Federal directives, line managers are free to grant access, as desired, once they are satisfied that they understand and are willing to accept the risks. This section gives line managers guidelines to follow so that they can understand and assess the risks that they are taking when they grant access to systems.

4.7.2. Who is Responsible for Granting Access?

Although System Administrators actually do the work required to allow users to access systems and software applications, line managers bear the ultimate responsibility for ensuring that the guidelines in this section are followed. Line managers should review all requests for access and apply the guidelines.

4.7.3. General Guidance for Granting Access

Line managers should grant the minimum privileges necessary for users to accomplish their tasks. Contracts, grants, international agreements, and position descriptions are all sources of information that may help determine an appropriate privilege level.

4.7.4. Categories of Users

This section provides separate guidelines for granting access to IT resources, based on user category. The following are the user categories referred to in these guidelines:

a. U.S. citizens and resident aliens.

b. Foreign nationals who are not international partners and who are hired by contractors in the normal course of business.

c. Foreign nationals who are international partners and who seek access to NASA's IT resources under the terms of an international agreement.

4.7.5. Types of Access

This document identifies the following types of access privileges:

a. Privileged access--Can bypass, modify, or disable the technical or operational system security controls.

b. Limited privilege access--Can bypass security controls for part of a system or application but not the entire system or application.

c. Non-privileged access--Cannot bypass any security controls.

4.7.6. Management Guidelines for Granting IT Access

Except for the general guideline that employees should be given the minimum access needed to accomplish their jobs, most managers do not have a consistent methodology for determining who may or who may not have access to their IT systems. This section provides some assistance to line managers in the form of questions to ask themselves before granting access. Granting access is a risk-acceptance process. Unless the applicant either requires screening or is a foreign national who is not an international partner and cannot be meaningfully investigated, managers need only be satisfied with the answers that they receive to the questions below.

4.7.6.1. Questions to Consider for All User Categories

a. Is there a valid requirement for access to the computer?

b. Does the individual understand the limits of access being granted?

c. Does the individual understand the restrictions and accountability that go with being granted a user ID? These include the following:

(1) Exploration of computer systems beyond authorized access areas is prohibited.

(2) Accounts will not be shared except as specifically authorized by management.

(3) Passwords used for identification of individual users may be shared only in accordance with the provisions in baseline requirements. (See appendix A)

(4) IT systems are provided for official NASA business.

(5) Users may be held liable for activities that occur, using their accounts.

(6) Depending upon the nature and severity of an offense, users may be subject to temporary or permanent loss of access privileges, disciplinary action, or civil or criminal prosecution under Federal or State law.

d. Is there any information on the computer or computers to which the individual will have access that is inappropriate for the individual to possess? (If so, adequate controls must be in place to prevent unlawful or improper access, or alternative arrangements must be made.)

e. Does the computer track and log security-relevant transactions sufficient to monitor user access limitations?

f. Does the individual understand that, by logging on to a NASA computer system, the user has granted permission for all of his or her activities in that system to be monitored and recorded?

g. Does the line manager acknowledge responsibility for granting access and acknowledge that granting access to this individual is in the best interests of NASA?

4.7.6.2. Special Questions to Consider for U.S. Residents

If the individual requires privileged access or access with limited system privileges, has an appropriate screening (e.g., personnel security investigation) been successfully completed?

4.7.6.3. Special Questions to Consider for Foreign Nationals Who Are Not International Partners

a. Is access requested only for a nonprivileged account? (Privileged access and access with limited system privileges are not authorized for foreign nationals who are not international partners.)

b. Is there any technological information on the computer system or computers to which the individual will have access that is export controlled under U.S. law? (If so, adequate controls must be in place to prevent unlawful access, or alternative arrangements must be made.)

4.7.6.4. Special Questions to Consider for International Partners

a. If the individual requires privileged access or access with limited system privileges, has an appropriate screening (i.e., personnel security investigation) been successfully completed? (NASA Headquarters handles investigations for all international partners. The names and privilege levels requested will be submitted through the CCS.)

b. Is there any technological information on the computer or computers to which the individual will have access that is export controlled under U. S. law or not approved for export under the individual's international agreement? (If so, appropriate security controls must be in place, or alternative arrangements must be made.)

4.7.7. System Administrators Guidelines for Granting IT Access

System Administrators shall require an Account Request Document for each user who requests access to a multiuser IT system. At a minimum, the Account Request Document will contain the following:

a. Requester's name, mailing address, telephone number, and affiliation (e.g., organization code, company name, university name, or other affiliation identification).

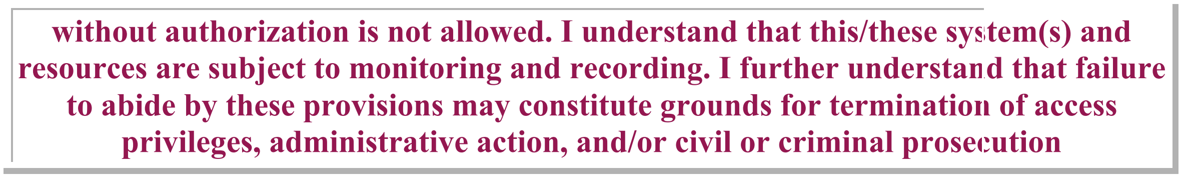
b. Requester's citizenship. If the citizenship is not that of the United States, then the requester must indicate his or her citizenship status, such as Permanent Resident Alien or Foreign National. Also, if the requester will not be accessing the system from within the United States, indicate from what country normal access will occur.

c. For non-Government employees, identification of the official relationship of the requester to NASA (e.g., grant, Memorandum of Understanding, contract, or other work agreement).

d. Identification of the system, or group of systems, for which an account is being requested.

e. Requester's signature and the date the requester acknowledges understanding and intention to comply with the acknowledgement statement in Figure 4-8:

> **Unauthorized use of the computer accounts and computer resources to which I am granted access is a violation of Section 799, Title 18, U.S. Code; constitutes theft; and is punishable by law. I understand that I am the only individual to access these accounts and will not knowingly permit access by others without written approval. I understand that my misuse of assigned accounts, and my accessing others' accounts**



without authorization is not allowed. I understand that this/these system(s) and resources are subject to monitoring and recording. I further understand that failure to abide by these provisions may constitute grounds for termination of access privileges, administrative action, and/or civil or criminal prosecution

Figure 4-8

f. Identification of the level of user privileges afforded to the account.

g. A Government management official's signature, such as a Branch Chief, Resource Monitor, Grant Monitor, data owner, or Contracting Officer's Technical Representative (COTR), that approves the legitimate need to access the systems to perform authorized Government activities. A Government designee may be appointed to sign in place of the Government management official.

4.8. Appropriate Use of Information Technology Resources

4.8.1. Overview

4.8.1.1. The following guidance is provided for the appropriate, ethical, and legal use of IT resources belonging to NASA. This section answers commonly asked questions about these topics and to give managers at all levels a common baseline for discussing these topics with their employees.

4.8.1.2. Laws concerning computers and computer crimes are constantly changing. To get the most recent information about laws related to computer crimes, consult the Center's Office of Chief Counsel. To get the most recent information about computer usage policy matters, contact the Human Resources Office, CIO, or Center IT Security Manager.

4.8.2. Official Business Use of Government Resources

NASA provides computer systems for the purpose of transacting official business. The following sections provide guidance on what is considered official business use, what is not considered official business use, and what use may be considered acceptable use with proper approval.

4.8.3. Official Business Uses

4.8.3.1. Official business broadly includes any computer processing that is required as part of the job. Official business includes, but is not limited to, the performance of NASA work-related duties in position descriptions, professional training and class work, work covered under grant agreements with NASA, tasks directed via NASA contracts, agreements with international partners, Center-authorized activities, and support activities related to NASA contract tasking.

4.8.3.2. With the concurrence of appropriate Center management, some less formal activities may be authorized. Authorization for such activities should be documented by management and may include, but not be limited to, the following:

a. Work-related events, such as a technical symposiums, classes, and presentations.

b. Activities sponsored by the Center, such as child care center and carpooling activities.

c. Events and activities specific to a particular NASA or Center organization.

d. Center-sanctioned activities, such as blood drives, sanctioned clubs, and organizations.

4.8.3.3. Management may permit some infrequent personal use of electronic mail. When communication cannot reasonably be made during non-business hours, employees may exchange brief messages with such persons or entities as the following:

a. Spouse or dependent.

b. Someone responsible for the care of a spouse or dependent.

c. State and local government agencies on personal matters.

d. Medical care providers.

e. Dentists.

f. Users may also use electronic mail in emergency situations.

4.8.4. Other Permissible Uses

4.8.4.1. Because there is no measurable cost, some limited personal use of Internet services, such as the World Wide Web and electronic mail, is permitted, provided it does not interfere with the employee's work or the work of others. Extreme care must be taken regarding content matter. Under no circumstances is it permissible to access or download material that would create a hostile or offensive work environment, such as racist or sexually explicit material. Use must be kept to brief periods when it can reasonably be assumed that the employee is in a nonduty status, such as during lunch breaks.

4.8.4.2. Some uses of NASA computer systems are clearly outside the boundaries of official business and permissible use. Prohibited uses of NASA's IT resources include using systems to do the following:

a. Maintaining or conducting an outside business.

b. Monitoring network traffic (e.g., run a sniffer); access IT resources; or copy data, files, or software without prior authorization. (Activities for which prior authorization is assumed include performing defined job duties, copying information that is intended to be copied, and doing work that has been approved by the Center IT Security Manager.)

c. Participating in Chat Rooms, News Groups, or similar activities where the posting will be seen by the public. Use of the NASA Internet address of "nasa.gov" is a representation of the Agency, analogous to the use of NASA letterhead in which the opinions expressed reflect on NASA.

d. Advertising goods or services for sale for monetary or personal gain.

e. Sending chain letters, personal mass mailings, hoaxes, or harassing messages.

4.8.4.3 Users should be particularly careful about using NASA computer systems in any way that could be interpreted as intending to influence any member of Congress to favor or oppose any legislation or appropriation. If the offender is an officer or employee of the United States, such an act may fall under a provision of Title 18 U. S. Code, Section 1913, "Lobbying with appropriated monies," which carries severe penalties upon conviction. If there are any questions about any aspect of this provision of law, contact your Center's Office of Chief Counsel for advice and assistance.

4.9. Software Usage

4.9.1. Overview

All users of NASA resources must comply with the terms of any license agreement for any software that NASA provides. It is usually illegal in the United States and most other countries to make or distribute copies of copyrighted material without authorization from the copyright holder. The NASA OIG, line managers, and other authorized individuals occasionally audit U.S. Government-owned equipment for the presence of unlicensed software. Each user is responsible for reading and complying with the terms of the license agreement that accompanies software.

4.9.2. Usage Guidelines by Software Type

The following are guidelines for appropriately using software:

a. Public Domain Software--Some software authors choose to make their software publicly available under terms that the author may specify. This public domain software may be used on NASA computers at the option of the line manager.

b. Shareware--Shareware is software that is available for a trial period at no cost. Users who wish to continue using shareware after the trial period may then be required to pay a license fee. Shareware is permitted on NASA computers at the option of the line manager, but the license fee must be paid.

c. Software Use at Home--Many users have workstations at home where they perform job-related work. Some software licenses accommodate use at home as well as at work. Some licenses may even permit personal home use of Government-purchased software. NASA allows users to make any legitimate use of a Government-purchased software package that is consistent with the license agreement. The burden is on the user to understand and to comply with that agreement.

d. Inspection of Imported Software for Malicious Code--All software entering the NASA community is called "imported software." Before being installed on any NASA-owned computer, all imported software must be approved by the responsible line manager. Each line manager may have a slightly different approval process, but all approval processes must include a check for the presence of malicious code, such as viruses, trap doors, and trojan code. Diskettes that users bring from home and diskettes that they bring back from travel have in the past been fertile sources of computer viruses. The use of imported software is permitted, but the user must take responsibility for examining it for the presence of malicious code before installing it. NASA and its immediate contractor community are required to have a process in place to inspect imported software. For more assistance, contact your organizational CSO.

4.10. Access Warning Banner, Notification of Rights, and Monitoring

4.10.1. Overview

Government computer systems may be targets of hostile activities and subject to other forms of unauthorized use. To counter these activities, the Government may monitor and record the use of Government computer systems through keystroke monitoring and other methods. To deter misuse and notify all users that their use may be monitored, guidance is provided on implementing a warning banner on all appropriate NASA computer systems. This direction applies to all NASA-owned or NASA-funded IT systems, regardless of location or user, including Government-provided equipment.

4.10.2. Notification to Users at Logon

4.10.2.1. A NASA standard banner shall be loaded onto all computer systems covered by this guidance so that it is affirmatively displayed at the time a user boots his or her system or is initially challenged for an authentication. Users without a "nasa.gov" domain address will see the NASA standard banner only when the NASA system they are attempting to access requires a user password identification.

4.10.2.2. Since new laws regarding employee expectations of privacy on employer IT resources are being tested in the courts and old laws are being applied in cases involving IT, consult the Center IT Security Manager for the latest NASA standard banner.

4.10.2.3. The NASA standard banner is intended as a minimal warning to effect the objectives described in the overview, above. In cases where there are reasons to deviate from, supplement, or not implement the standard banner, such exceptions shall be approved by the Center CIO or designee and concurred in writing by the servicing Chief Counsel (in the case of Headquarters, Office of the General Counsel) and local Inspector General. Line managers should work through their assigned legal counsel to seek the advice and concurrence of their local Inspector General. The Center IT Security Manager shall maintain documentation for approved exceptions.

4.10.3. Notification of Rights to IT Resources

4.10.3.1. All NASA computer systems, like all systems that belong to the U. S. Government, are subject to audits. Users should realize that they do not have any expectation of privacy when they use a NASA computer system.

4.10.3.2. Every user of a NASA-owned computer system should understand that the computer equipment, software, and information they contain are not their property. They are the property of the U.S. Government, a cooperating foreign government, corporate entity, research center, university, or other entity as specified in the agreement or contract that originally permitted access to the system.

4.10.4. Monitoring of IT Resources

4.10.4.1. All activities on NASA's computer systems may be monitored to the extent permitted by law and NASA directives. This monitoring may include traffic analysis, keystroke monitoring, examination of log files, and examination of any or all files on the computer. Monitoring may be initiated any time evidence of apparent misuse or possible criminal activity has been reported.

4.10.4.2. All files in a user's account, including electronic mail, may be examined under appropriate circumstances by the following staff:

a. Line manager.

b. Officials representing the Center CIO.

c. Director of Human Resources.

d. Office of Chief Counsel.

e. Representatives from the CCS.

f. Representatives of the OIG.

g. Other law enforcement officials.

4.10.5. Notice of Information Gathering

If a system (e.g., WEB pages or News Groups) is gathering information on an individual's identity or activities, the system must provide a warning, notifying the individual what information is being collected and what will be done with the information. Gathering statistical data (e.g., usage, domains, traffic loading) not identified with an individual is permitted. For guidance see the Center IT Security Manager.

4.11. Use of Encryption Technology

The ability to limit system access to authorized individuals and to transmit information securely, i.e., so that if a communication is intercepted the information is still unintelligible and any unauthorized changes made in transit are detected by the receiver, is essential for ensuring the availability, confidentiality, and integrity of NASA IT systems and data. The discipline known as Communications Security (COMSEC) is required for the protection of classified information. (Consult the Center Security Officer, the DAA, or the NASA Security COMSEC Handbook for guidance.) For unclassified information, it is NASA policy to comply with national policy by ensuring that all of our valuable information and critical systems are afforded an adequate degree of protection that is commensurate with the risks posed to NASA IT resources and the magnitude of potential harm that could be experienced by the Agency if the IT resources should be compromised.

4.11.1. General Guidance for Using Encryption Technology for Unclassified Systems

For unclassified information, the Agency depends largely on traditional password-user identification to protect access to its IT resources. This methodology has become vulnerable. The Agency must now consider employing encryption technology to protect all of its IT resources from unauthorized access and exploitation during transmission. When doing a risk assessment, it is essential that line managers and data owners document and justify their decision to use encryption technology or to accept the risk of not encrypting and the risk of exposure to compromised access and transmission interceptions.

4.11.1.1. When the determination is made that encryption will be used, line managers and data owners of unclassified systems shall comply with all applicable Federal Information Processing Standards (FIPS) and/or National Security Agency (NSA) requirements for encrypting Government-owned IT resources that are in a production mode of operation or, if not in a production mode of operation, represent high-value assets to the Agency. Currently, for FIPS-approved products, this means using the Data Encryption Standard (DES) in accordance with FIPS 140-1, General Security Requirements for Equipment Using the Data Encryption Standard. Changes to the FIPS-approved product set are expected over time; therefore, the latest FIPS documentation should be consulted when determining if a specific product has been approved.

4.11.1.2. Using or not using encryption technology will be a risk-management decision, based upon a risk assessment of the threats, vulnerabilities, and potential harm that could be experienced by the Agency. Because of constant advances in technology and cryptanalysis techniques, even some forms of encryption that are FIPS approved, e.g., 40 bit DES, are considered to be weak for some applications. Therefore, the risk-assessment process must also result in a decision on the strength of encryption appropriate for the application, including allowance for increased encryption-breaking capability over the anticipated life of the system.

4.11.1.3. For production or high-value IT systems using encryption technology, procedures for key management, appropriate to the encryption technology adopted and associated Federal policy, will be established. As an example, for Public Key Infrastructure solutions, key management procedures will address key recovery, secure key exchange, and revocation of individual keys.

4.11.2. Detailed Guidance for Using Encryption for Classified and Unclassified Systems

The use of encryption technology will be addressed as part of each NASA Program Commitment Agreement (PCA). The decision to use encryption must be accompanied by a determination of the type, level, and strength of the encryption that will be used. Type refers to National Security Agency (NSA) or FIPS approved/endorsed; level refers to the Security Levels defined in FIPS PUB 140-1; and strength refers to the resistance of the encryption algorithm to attack and the length of the keys used with the algorithm (longer keys are stronger). At a minimum, the following will be integrated into all NASA space and aeronautic flight programs, IT systems, and tests:

a. Telemetry and Telecommunications Involving National Security Information (Classified):

(1) NSA-approved and endorsed encryption products and/or techniques will be applied to all telemetry and telecommunications involving national security information processed by NASA.

(2) There will be no waivers/variances/exceptions to this requirement. (See NPG 1600.6x for complete guidance.)

b. Command/Destruct Uplinks To Launch Vehicles, Spacecraft, Test Aircraft, and Other Manned Or Unmanned Aerospace Vehicles:

(1) Command Destruct Systems (CDS) should not be susceptible to any unauthorized and/or inadvertent radio transmissions or signals. To ensure that CDS respond only to authorized commands, secure CDS should be utilized. NSA and/or NIST-approved or endorsed techniques and products will be used to secure CDS.

(2) Exceptions to the policy to use secure CDS may be granted by the organization responsible for the safe conduct of launch operations. All exceptions must be reported to the Associate Administrator for Management Systems. Waivers/variances/exceptions to

the requirement to use NSA and/or NIST products will be considered on a case-by-case basis and approved by the Associate Administrator for Management Systems with concurrence by the NASA CIO.

c. Command and Control Links to Vehicles for Vehicle Housekeeping Activities:

(1) The need for and means to protect command/control uplinks will be determined through risk and cost assessments by the responsible program management in coordination with the NASA Security Management Office and the NSA. If encryption is required, these assessments will also determine the level, strength, and type of encryption system to be used. Only NSA and/or NIST-approved encryption products will be used to protect command and control uplinks.

(2) Waivers/variances/exceptions to the requirement to use only NSA and/or NIST-approved or endorsed products and techniques will be considered on a case-by-case basis and approved by the Associate Administrator for Management Systems with concurrence by the NASA CIO.

d. For Payload Operations Including Command and Control of the Payload and the Handling of Raw Data from Orbiting Payloads):

(1) Risk and cost assessments will be conducted by program/project management to determine if encryption is required and, if so, the level, strength, and type of encryption that would be most appropriate. Based on these assessments NSA and/or NIST-approved and endorsed encryption products and/or techniques will be used to protect payload data links, if encryption is required.

(2) Waivers/variances/exceptions to the requirement to use only NSA and/or NIST-approved or endorsed encryption products and/or techniques will be considered on a case-by-case basis and approved by the NASA CIO with concurrence by the Associate Administrator for Management Systems.

e. Business and Restricted Technology (BRT) Information Systems:

(1) Analysis will be conducted to determine if there are encryption requirements. If encryption requirements exist, risk and cost assessments will be conducted to determine the level and strength of encryption that would be most appropriate. Based on these assessments, NIST-approved and endorsed products and/or techniques will be used to protect data during telecommunications processes.

(2) Waivers/variances/exceptions to the requirement to use only NIST-approved and endorsed encryption products and/or techniques for general purpose administrative system encryption requirements will be considered on a case-by-case basis and approved by the NASA CIO.

4.11.3. Guidance for Requesting a Waiver

Variations from the encryption requirements described in paragraph 4.11.2 require a written waiver request addressed to the Associate Administrator for Management Systems or to the NASA CIO, as appropriate, and be approved by the appropriate Center Director prior to submission. (See paragraph A.5.2 for additional information on waivers to FIPS PUB 140-1 requirements.) The waiver request must include the following:

a. Name, location, and short description of system or application.

b. Short description of the nature of the data (e.g., vehicle command and control; payload command, control, data download or data upload; business and restricted technology; or, other sensitive information).

c. Nature of waiver requested (description of risk and control measure).

d. Time limit for which the waiver is needed.

e. Actions planned to be taken to remedy the situation that initiated the waiver request.

f. Alternatives considered to satisfy the requirement and provide an equivalent degree of protection. (Include a statement explaining why a waiver is being requested in lieu of the alternatives.)

4.12. National Security Information

4.12.1. Overview

"National security information" is information that could reasonably be expected to cause damage to national security upon unauthorized disclosure. Executive Order (EO) 12958 tasks the National Security Council with overall policy direction for classified information. The Secretary of Defense is the Executive Agent, and the Director, NSA is the National Manager for handling classified information in computers. The authority to declare information classified has been granted to selected Federal agencies, including NASA. This "classified" information falls into one of three classifications - confidential, secret, or top secret.

4.12.2. Elements in the IT Security of National Security Information

The following are key elements in the IT security program for national security information:

a. Designated Approval Authority (DAA)--A Designated Approval Authority will be appointed at each NASA Center. Each DAA will be knowledgeable in computer and networking technology as well as security methods and practices. DAA should not have a program or project interest in the facility and systems they accredit for processing national security information.

b. Accreditation--DAA accreditation of a facility and its systems will be based upon certification by the data owner and facility manager; a review of the Security Operations Plan (SOP) for the facility and systems; and verification and inspection of the protective measures and procedures of both the facility and systems being accredited, as appropriate.

c. Certification--The data owner and facility manager will certify that the protective measures and procedures described in the SOP for the facility and systems meet the requirements of the National Industrial Security Program Operating Manual Supplement (NISPOMSUP), as adopted by the DAA.

d. Security Operations Plan (SOP)--A SOP will be written as described in the NISPOMSUP and adopted by the DAA for NASA Centers' use. Deviations must be addressed, and any risk exposure must be specifically identified.

4.12.3. Guidance

The following guidance applies to national security information:

a. All NASA computer and networks handling national security information will be certified by the data owner, facility manager, IT Security Manager, and the CCS and accredited by a NASA DAA or by another duly appointed Federal DAA.

b. The policies and procedures for handling classified information outside of computers and networks are in the NPG 1620, NASA Security Guideline.

c. Although NASA's handling of national security information is generally consistent with those of other agencies, computers or networks that contain information classified by another Federal agency are bound by the policies and procedures specified by that agency and documented in agreement with the DAA.

d. Special programs, projects, or customers may impose additional protective measures beyond those approved by the NASA DAA.

CHAPTER 5. Information Technology (IT) Security Documentation

Documentation plays an important role in the NASA IT Security Program by serving as a tool for reporting the status and accomplishments of IT security, describing planned IT security activities, and substantiating that appropriate security measures have been taken. (See Figure 5-1.) This chapter describes the following four IT security documents and suggests the organization and content of each of these documents:

a. IT Security Plans for general support systems.

b. IT Security Plans for "major application" systems.

c. Center IT Security Plans.

d. IT Security Contingency Plans.

Although this chapter focuses on the four documents listed above, Centers and organizations may require additional documentation to meet their specific needs. Centers and organizations may set their own guidelines for any additional documentation that they require.

Figure 5-1

5.1. IT Security Plans

5.1.1. Description

An IT Security Plan is the logical result of the IT security planning process. (See Figure 5-2.) It provides key information about a system and describes the associated risks, the controls in place to counter risks, any risks that have not been addressed, and justification for not addressing risks. All of the information included in an IT Security Plan correlates to the outcome of steps from the IT security planning process.

Unless stated otherwise, the term "system" may refer to a single computer, a collection of computers with the same function and similar security needs (such as all the desktop computers, servers, and printers in a building or office), a software application (such as an accounting and payroll application), a network (including its supporting routers, controllers,

servers, and computers), or a functional entity that performs a specific task (e.g., wind tunnel IT controls, application servers, or mission control complexes, which may be composed of computers, networks, routers, and servers).

Figure 5-2

5.1.2. Requirement

5.1.2.1. An IT Security Plan is requiredfor all systems. Although separate IT Security Plans are required for support systems and the "major applications" processed by support systems, those who prepare these plans (e.g., line managers for support systems and data owners of the applications) should coordinate their efforts due to the shared risks. For example, the risks documented in an IT Security Plan for a support system could raise concerns for the data owner of an application processed on the support system. Likewise, an application that allows online collaboration with users in other countries could raise concerns for the line manager of a support system.

5.1.2.2. Figures 5-3 and 5-4 provide the outline and guidance for completing the IT Security Plan for General Support Systems and "major application" systems.

5.2. Center IT Security Plan

5.2.1. Description

A Center IT Security Plan provides a management summary of a Center's IT Security Program. This plan describes activities and accomplishments for the previous fiscal year, planned activities for the current fiscal year, and future activities for the upcoming fiscal year.

5.2.2. Requirements

Annually, the Center IT Security Manager and the CIO will prepare a Center IT Security Plan. The Center IT Security Manager will submit this plan to the Center Director or designee for approval. Figure 5-5 provides the outline and guidance for completing the Center IT Security Plan.

5.3. IT Security Contingency Plans

5.3.1. Description

An IT Security Contingency Plan describes the arrangements that have been made and the steps that will be taken to continue system operations in the event of a natural or human-caused disaster.

5.3.2. Requirements

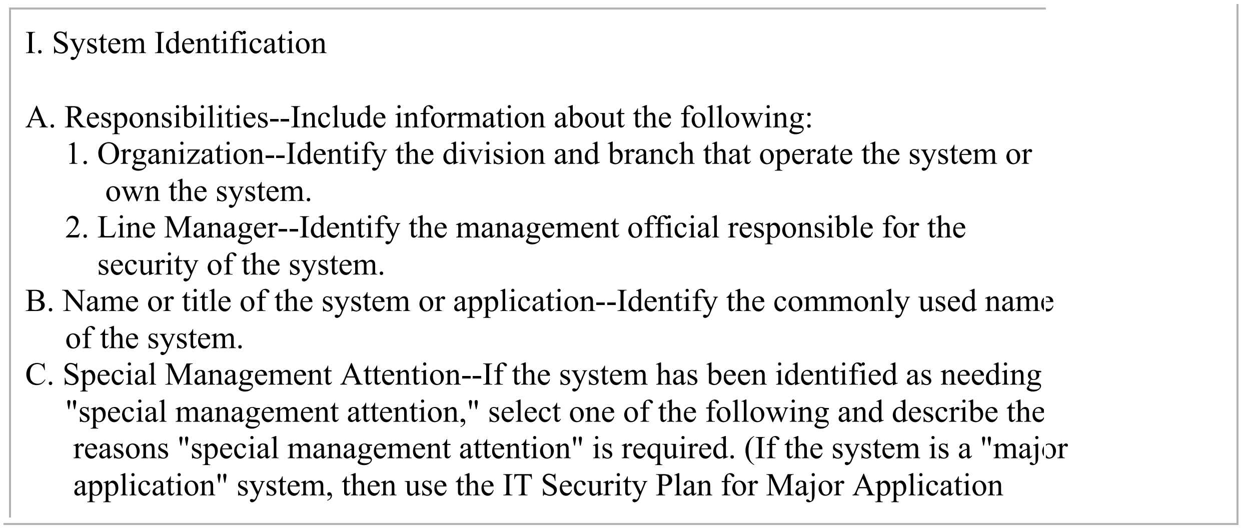
Each system must have an IT Security Contingency Plan. This plan must be reviewed and tested periodically (at least every 3 years or upon significant change). At the line manager's option, and depending on the size and complexity of the system, the plan may appear as a section of the IT Security Plan or it may be issued as a separate document. A copy of the plan should be kept at a location away from the system (at a minimum in another building), usually with the backup materials, in case it is not possible to return to the facility. The scope, extent, and expected time to restore to full processing capability must be clearly defined so that system users can plan appropriately. Figure 5-6 provides the outline and guidance for completing the IT Security Contingency Plan.

5.3.3. Special Considerations for Contingency Planning

5.3.3.1. Those responsible for managing the applications that run on the system (and the data owner being supported) must plan ways that their data or application will continue performing critical functions if the facilities in which processing normally occurs suddenly become unable to support the application. Due to different recovery requirements, a separate IT Security Contingency Plan may be required for each application.

5.3.3.2. If the system in question provides services outside the system's own organization, the IT Security Contingency Plan must be coordinated with those receiving services. Those receiving services will need to know how long they can expect the system to be unavailable, what initial level of service will be restored, and how they will be kept informed of the system's operational status.

Figure 5-3 (Part 1 of 6)
IT Security Plan for General Support Systems



I. System Identification

A. Responsibilities--Include information about the following:
  1. Organization--Identify the division and branch that operate the system or own the system.
  2. Line Manager--Identify the management official responsible for the security of the system.

B. Name or title of the system or application--Identify the commonly used name of the system.

C. Special Management Attention--If the system has been identified as needing "special management attention," select one of the following and describe the reasons "special management attention" is required. (If the system is a "major application" system, then use the IT Security Plan for Major Application systems.)

1. Major Information System--A system that has been designated by the Chief Information Officer as a "major information system" for OMB A-11 reporting.
2. Mission Critical System--A system that provides Agencywide support, such as a wide area network, Agencywide business function, command and control of space system, Agencywide consolidated computer resource, or computer resource that affects life support.
3. NASA Resource Protection (NRP) Facility--A computer resource that is critical to a facility or operation as designated under the NRP program by the cognizant Program Office (Reference: NPD 1600.2, NASA Security Program.)
4. Center Designated--Other computer systems that the Center Director or Chief Information Officer has designated as requiring "special management attention."

D. Operational status--Indicate whether the system or application is currently operational or nonoperational (e.g., being designed, developed, procured, implemented, or modified).

Figure 5-3 (Part 2 of 6)
IT Security Plan for General Support Systems

E. General description/purpose--Include the following information in narrative format with attachments for lists and drawings:

1. Make and model of major hardware components
2. Major uses or functions (e.g., modeling, simulations, accounting, analysis)
3. Network access and connectivity
4. System software and versions and the software applications running on the system
5. Operated by Government or contractors (owned or leased)
6. Hours of operation
7. Number of user accounts and type of user (e.g., researchers, programmers, administrative support).

F. Processing environmental and special considerations--Include information such as the following in narrative format:

1. Critical processing periods (e.g., end of month, pay day)
2. Indication of whether the system serves a large number of offsite users, such as university students, other agencies, or foreign nationals
3. Description of other systems/application that interface with the system.

G. Information contacts--Provide the names, telephone numbers, mail stops, and electronic mail addresses of the following individuals:

1. Organization Computer Security Official (or Project /Program Manager,

especially if the system is under development)

2. Line manager
3. System Administrator
4. Other technical contacts (e.g., staff who support the System Administrator)

II. Information Identification

A. Information processed--Describe the information processed (e.g., payroll, accounting, safety, command and control, network support, experiment results, calculations, software for unmanned flight, simulation software, procurement).

Figure 5-3 (Part 3 of 6)
IT Security Plan for General Support Systems

B. Category--Identify the type of information processed. (See paragraph 4.2.9 for a description of these information categories). The category will determine some of the baseline controls needed to protect the information.

1. Mission (MSN)
2. Business and Restricted Technology (BRT)
3. Scientific, Engineering, and Research (SER)
4. Administrative (ADM)
5. Public Access (PUB)

C. Applicable laws, policies, and guidance affecting the information--List any specific standards, guidance, or policies that require security measures to be used to protect information on the system. Some examples are Privacy Act of 1974, Federal Managers' Financial Integrity Act, Trade Secrets Act, Patent and Trademark Laws, Export Control Laws, and The Accounting and Auditing Act. Include NASA and Center policies and guidance in the list.

D. Impact of loss of system and/or data--Describe the potential impacts if the system, software applications, or the information processed is altered, destroyed, or unavailable (i.e., at what point does the loss become a high priority-1 hour, 1 day, 1 week, or 1 month?). Discuss the loss of data, loss of processing time, recovery cost for hardware and software (i.e., programs), impact to budgets, impact to customers, and estimated recovery time.

E. System value--Estimate the replacement cost for the hardware and software programs that comprise the system. Be sure to include the cost of rebuilding databases and programming code if they are not backed up or they are not remotely located.

III. Information Sharing--Describe the information to be shared with external customers. (External customers include any Federal, State, or local governments, international partners, other NASA organizations, or organizations in the private sector.) Identify the intended recipients, the controls that will be used, and any applicable policies or laws that must be followed.

IV. Risk Assessment and Analysis

A. Summarize the findings of the risk assessment performed on the system. Include when the risk assessment was done, who conducted it, and who approved it.

B. Describe the results of the risk analysis, the chosen controls, and any residual risks. Indicate the possible effects these risks could have.

C. Document any baseline requirements that are not being met and indicate why the requirement is not being met or why it is not applicable. (See appendix A for the list of baseline requirements.)

Figure 5-3 (Part 4 of 6)
IT Security Plan for General Support Systems

V. Technical Controls--Summarize the technical controls that enforce the rules or policies of the system (e.g., the ability to force password changes at predetermined intervals). These controls include those that meet baseline requirements and any additional controls found to be necessary during the risk assessment.

VI. Public Access Controls--If general public access is allowed, describe how the information, software applications, and systems will be protected against loss, alteration, unavailability, or unauthorized disclosure, as appropriate.

VII. Rules of the System--Define the responsibilities of all persons who have access to the system, both privileged and unprivileged users. The rules should take into consideration the needs of all parties who use the system. They should be as strict as necessary to ensure that security is not compromised. The rules for use of the system will be based on the results of the risk analysis. Among the topics the rules should cover are the following:

A. Process for obtaining an account

B. Process for accessing the system from home or while on travel

C. Kinds of information that may be stored on the system and the authorized uses to which that information may be put

D. User privileges and limitations

E. User authentication

F. Process for restoring service from system crashes or maintenance

G. Process for escorting personnel who do not have access to the system

H. Consequences for failure to follow the rules

VIII. Personnel Screening --Indicate the level of screening required for privileged users and limited privilege users who can bypass security processes and controls. Include the number of privileged and limited privilege users.

IX. Training--Indicate whether users of the system receive training on the following topics:

A. Rules of the system

B. Responsibilities described in chapter 2

C. How to detect and respond to suspected IT security incidents

D. How to get help in using the system or its security features

E. Center policies, procedures, and guidelines

Figure 5-3 (Part 5 of 6)
IT Security Plan for General Support Systems

X. Contingency Planning--A plan for continuing operations in the case of a natural or human-caused disaster must be established and tested. Indicate whether an up-to-date contingency plan exists. If a contingency plan exists, list the date it was last tested. The plan must be reviewed and tested periodically. At the manager's option, depending upon the size and complexity of the system, the contingency plan may appear as a section of the security plan or be issued as a separate document, but it should be attached to the plan. If the constituents of the system are one or more applications that are run in a system furnished by another organization, the application manager's job is to plan how the application will continue performing its critical functions if the facilities in which processing normally occurs suddenly become unable to support the application. Also, indicate the estimated time required to return to full processing capability.

XI. Incident Response--Describe how security incidents should be reported through the management chain for this system or application. Identify the names and telephone numbers of people who should be called if a security incident is discovered. If special incident response procedures are required, include them in this section.

XII. System Interconnection--Describe the connectivity with other IT systems. Discuss how the access to and from other systems is controlled to an acceptable degree of risk. If users of this system have limitations to external access, these limitations should be described in this section and should be consistent with the system rules. There are various degrees of system interconnection that management may choose to permit. A management decision to permit connectivity must be based upon the availability of appropriate safeguards and the degree of residual risk. Connectivity may not be attempted until the risk assessment indicates that the risks posed to the system are acceptable and that the line manager has assured that this system poses no undue risk to others sharing common facilities. Describe the coordination that has taken place with other managers who share common resources. Document any concerns about risks. If the risks are acceptable, the author of the plan will document acceptance of these risks.

Figure 5-3 (Part 6 of 6)
IT Security Plan for General Support Systems

XIII. Review of Security Controls--Describe the process for performing an independent review of the security controls of the system. This review is required at least every 3 years or upon significant changes.

XIV. Authorization to Process--Ensure that the responsible line manager authorizes in writing the use of the system by confirming that, as implemented, this IT Security Plan adequately secures the system. For systems requiring "special management attention," the Center CIO must also sign, authorizing the system to process. This authorization can be a cover letter attached to the plan or a signed statement at the end of the document. This authorization must clearly state that the manager finds that the IT Security Plan adequately secures the system, its data, and its operation.

Figure 5-4 (Part 1 of 5)
IT Security Plan for "Major Application" Systems

I. System Identification

A. Responsibilities--Include information about the following:

1. Organization--Identify the division and branch that operate the system or own the "major application" system.
2. Line Manager--Identify the management official responsible for the security of the "major application" system.

B. Name or title--Identify the commonly used name of the "major application" system.

C. Special Management Attention--As a "major application" system, "special management attention" is required due to the risk and magnitude of harm that would result from the loss, misuse, or unauthorized access to or modification of the information in the application.

D. Operational status--Indicate whether the system is currently operational or nonoperational (e.g., being designed, developed, procured, implemented, or modified).

E. General description/purpose--Include the following information in narrative format with attachments for lists and drawings:

1. Major uses or functions (e.g., modeling, simulations, accounting, analysis)
2. Network access and connectivity
3. System software and versions and the application software running on the system
4. Operated by Government or contractors (owned or leased)
5. Hours of operation
6. Number of user accounts and type of user (e.g., researchers, programmers, administrative support)

F. Processing environment and special considerations--Include information such as the following in narrative format:

1. Critical processing periods (e.g., end of month, pay day)
2. Indication of whether the system serves a large number of offsite users, such as university students, other agencies, or foreign nationals
3. Describe other systems/applications that interface with the system

Figure 5-4 (Part 2 of 5)
IT Security Plan for "Major Application" Systems

G. Information contacts--Provide the names, telephone numbers, mail stops, and electronic mail addresses of the following individuals:

1.Organization Computer Security Official (or Project /Program Manager, especially if the system is under development)
2. Line manager
3. System Administrator
4. Other technical contacts (e.g., staff who support the System Administrator)

II. Information Identification

A. Information processed--Describe the information processed (e.g., payroll, accounting, safety, command and control, network support, experiment results, calculations, software for unmanned flight, simulation software, procurement).

B. Category--Identify the type of information processed. (See paragraph 4.2.9 for a description of these information categories.) The category will determine some of the baseline controls needed to protect the information.

1. Mission (MSN)
2. Business and Restricted Technology (BRT)
3. Scientific, Engineering, and Research (SER)
4. Administrative (ADM)
5. Public Access (PUB)

C. Applicable laws, policies, and guidance affecting the information--List any specific standards, guidance, or policies that require security measures to be used to protect information on the system. Some examples are Privacy Act of 1974, Federal Managers' Financial Integrity Act, Trade Secrets Act, Patent and Trademark Laws, Export Control Laws, and The Accounting and Auditing Act. Include NASA and Center policies and guidance in the list.

D. Impact of loss of system and/or data--Describe the potential impacts if the system, application, or the information processed is altered, destroyed, or unavailable (i.e., at what point does the loss become a high priority-1 hour, 1 day, 1 week, or 1 month?). Discuss the loss of data, loss of processing time, recovery cost for hardware and software (i.e., programs), impact to budgets, impact to customers, and estimated recovery time.

E. Major Application's Value--Estimate the replacement cost for the software programs that comprise the application. Be sure to include the cost of rebuilding databases and programming code if they are not backed up or they are not remotely located.

Figure 5-4 (Part 3 of 5)
IT Security Plan for "Major Application" Systems

III. Information Sharing--Describe the information to be shared with external customers. (External customers include any Federal, State, or local governments, international partners, other NASA organizations, or organizations in the private sector.) Identify the intended recipients, the controls that will be used, and any applicable policies or laws that must be followed.

IV. Risk Assessment and Analysis

A. Summarize the findings of the risk assessment performed on the system. Include when the risk assessment was done, who conducted it, and who approved it.
B. Describe the results of the risk analysis, the chosen controls, and any residual risks. Indicate the possible effects these risks could have.
C. Document any baseline requirements that are not being met and indicate why the requirement is not being met or why it is not applicable. (See appendix A for the list of baseline requirements.)

V. Technical Controls--Summarize the technical controls that enforce the rules or policies of the major application system (e.g., the ability to force password changes at predetermined intervals). These controls include those that meet baseline requirements and any additional controls found to be necessary during the risk assessment.

VI. Public Access Controls--If general public access is allowed, describe ways the information, data, and application software will be protected against loss, alteration, unavailability, or unauthorized disclosure, as appropriate.

VII. Major Application Rules--Define the responsibilities of all persons who have access to the system, both privileged and unprivileged users. The rules should take into consideration the needs of all parties who use the "major application" system. They should be as strict as necessary to ensure that security is not compromised. The rules for use of the system will be based on the results of the risk analysis. Among the topics the rules should cover are the following:
A. Process for obtaining an account
B. Process for accessing the system from home or while on travel
C. Types of information that may be stored on the system and the authorized uses to which that information may be put
D. User privileges and limitations

Figure 5-4 (Part 4 of 5)
IT Security Plan for "Major Application" Systems

E. User authentication
F. Process for restoring service from crashes or maintenance
G. Process for escorting/monitoring personnel who do not have access to the system
H. Consequences for failure to follow the rules

VIII. Personnel Screening--Indicate the level of screening required for privileged users and limited privilege users who can bypass security processes and controls. Include the number of privileged and limited privilege users.

IX. Specialized Training--No user will be permitted access to a critical system without having been appropriately trained. The plan should accommodate training geared to the privileges of the position that the individual will assume. Some of the training needs will derive from the risk analysis. The plan should include at least the following:
A. Responsibilities described in chapter 2
B. Rules of the system
C. How to detect and respond to suspected IT security incidents
D. How to get help in using the "major application" system and its security features
E. Center policies, procedures, and guidelines

X. Contingency Planning--A plan for continuing operations in the case of a natural or human-caused disaster must be established and tested. Indicate whether an up-to-date contingency plan exists. If a contingency plan exists, list the date it was last tested. The plan must be reviewed and tested periodically. At the manager's option, depending upon the size and complexity of the system, the contingency plan may appear as a section of the security plan or be issued as a separate document, but it should be attached to the plan. If the constituents of the system are one or more applications that are run in an system furnished by another organization, the application manager's job is to plan how the application will continue performing its critical functions if the facilities in which processing normally occurs suddenly become unable to support the application. Also, indicate the estimated time required to return to full processing capability.

XI. Incident Response--Describe how security incidents will be reported through the management chain and to the local IT Security Manager. Identify the names and telephone numbers of people who should be called if a security incident is discovered. If special incident response procedures are required, include them in this section.

Figure 5-4 (Part 5 of 5)
IT Security Plan for "Major Application" Systems

XII. Information Sharing--Identify any security risks to which the application is exposed because of the support system on which it is running or because information is shared with any Federal, State, or local governments, shared with international partners, shared internally to NASA, or shared with organizations in the private sector. Controls on the information may need to vary considerably, depending on the entity with which the information is shared. Information labeling or formal agreements as to the further disposition of the information may be required. This section of the plan should list the kinds of information to be shared, the intended recipients, and the controls that will be used for each category. Document any concerns about the risks. If the risks are acceptable, the author of the plan will document acceptance of these support system risks.

XIII. Review of Security Controls--Describe the process for performing an independent review of the security controls of the application. This review is required at least every 3 years or upon significant changes.

XIV. Authorization to Process--Ensure that the responsible line manager and the Center CIO authorizes in writing the use of the "major application" system by confirming that, as implemented, this IT Security Plan adequately secures the "major application" system. This authorization can be a cover letter attached to the plan or a signed statement at the end of the document. This authorization must clearly state that the manager finds that the IT Security Plan adequately secures the "major application," its data, and its operation.

Figure 5-5 (Part 1 of 1)
Center IT Security Plan

I. Executive Summary--Describe the goals and philosophy of the Center's IT Security Program. List and describe the primary areas of focus for the fiscal year applicable to this plan (i.e., the current fiscal year).

II. Introduction--Provide an overview of the Center's IT Security Program by discussing the following:

A. Purpose
B. Scope

C. Organization structure

III. Goals and Objectives--List and describe each of the goals and objectives of the Center's IT Security Program.

IV. Summary of Incidents--Summarize and describe the impact of the IT security incidents that occurred for the past fiscal year.

V. Significant IT Security Activities--Describe the IT security activities from the previous fiscal year, the expected activities for the current fiscal year, and future activities for the following fiscal year. As appropriate, discuss the following topics in the summary for each fiscal year:

A. IT Security Plans
B. Organization and management support
C. IT security reviews
D. IT security awareness and training
E. IT security technical controls
F. Account management
G. Automated audit tools
H. Management of classified information
I. Management of export controlled information
J. Contingency and recovery planning
K. IT Security life-cycle requirements

VI. IT Security Program Management--Describe the budget, project staffing, and expected milestones for the current fiscal year.

VII. Center Systems--Provide a list of the systems at the Center that are not classified and a list of those that are classified.

Figure 5-6 (Part 1 of 2)
IT Security Contingency Plan

I. Overview--Describe the scope of the contingency plan, instructions on how to use the plan, and identify the applications that the plan would include in the restoration process.

II. Assumptions--Describe the circumstances under which the plan will be invoked. State the maximum acceptable outage limit (e.g., processing must be re-established within 6 hours). Identify the name and location of the organization that will provide alternate processing facilities in the event of a system failure.

III. Recovery teams--List the members of the recovery team (or teams). Include the names of appointed leaders, each member's assigned duties, and contact information for each member.

If there is more than one recovery team, include a description of the responsibilities each team has during the recovery.

IV. Staffing--Describe plans for having staff available at a backup location. Include the funding sources to cover travel, lodging, per diem, overtime, and other associated costs.

V. Vendors--List the vendors, suppliers, and support service contracts normally used in processing. Include contact information for each. Arrangements should be made with vendors in advance for the delivery of equipment in the event of a disaster. If preexisting arrangements are not made, the time required to deliver, install, and start up new equipment/software may exceed the allowable timeframes required for recovery.

VI. Current locations of vital records--Include the location of any currently used off-site facilities that store vital records needed to get the system back into operation. List the names and contact information for the personnel who have access to these facilities and include information on how to contact them at the off-site storage location. If appropriate, provide maps that give directions to these facilities.

VII. Restoration procedures--Describe the procedures for restoration, including procedures for downloading restored data to servers and workstations from backups, communication links, restoring power, and testing. All restoring procedures need to identify the acceptable level of security (both physical and logical) and document any risks resulting from the recovery, including those at an alternative processing site.

Figure 5-6 (Part 2 of 2)
IT Security Contingency Plan

VIII. Inventory--Identify all vendor software running on the system. Include the names of persons to contact for support. Identify any critical materials stored off-site that will be required for getting the system back online or for processing on a backup system elsewhere.

IX. Movement of vital records--Identify any hardcopy documents that should be gathered and moved to the backup site to facilitate recovery and operations. Consider keeping copies of these materials prepackaged at the backup site or at another appropriate offsite location.

X. Contracts--Include copies of any contracts or agreements for any backup sites for processing, hardware or software maintenance, copies of leases, and license information. Also, include a copy of the offsite storage facility contract.

XI. Equipment--If equipment is to be moved as a part of this plan, include all necessary configuration information for restoring the system at the backup site. Include instructions on packing and pre selected qualified movers. If the backup site has the equipment that will be used, include a copy of the agreed upon configuration at the backup site.

XII. Connectivity--Include lists and diagrams of required connectivity. State how voice communications will be maintained with management and customers.

XIII. Test procedures--List the procedures that will be used periodically to test the contingency plan. Test procedures should be comprehensive, including but not limited to the compatibility of alternate facilities equipment and software; the restoration and operation of systems software, communications facilities, and critical application systems at the alternate site; and the availability and currency of off-site backup of program and job execution language libraries.

The scope of the tests should address partial and total disasters at both peak and nonpeak processing periods. Users should be involved in testing high-priority application systems restoration and alternate facilities operation. Test objectives, scope, and results should be documented and attached to the contingency plan.

XIV. Modification--Identify the person assigned to make modifications to the plan, how often the list of contracts will be reviewed, and the person approving the changes.

XV. Distribution--Identify everyone on the distribution list for the plan so that updates can be issued.

APPENDIX A. Baseline Information Technology (IT) Security Requirements

The tables in this appendix list the minimum technical, procedural, and physical IT security requirements for protecting NASA's IT resources. These requirements will help managers determine the controls that are needed for computer systems under their oversight.

A.1. Baseline Requirements

Baseline requirements are sets of technical, procedural, and physical IT security measures intended to ensure a reasonable level of security for a system. They are derived from "best practices" used by industry and the Government.

A.2. Use of Baseline Requirements

Baseline requirements are used in security planning as a benchmark for identifying risks to which a system may be exposed. The degree of compliance with these requirements is indicated in the IT Security Plan for the system. These requirements are also used in the definition phase of the system life-cycle process to ensure that an acceptable level of security is built into a system.

A.3. Baseline Requirements and Information Categories

Baseline requirements vary, depending on the information category of the system (see Figure A-1). The information categories, their abbreviations, and descriptions are as follows:

Categories of NASA Information

MSN
Mission
BRT
Business and
Restricted
Technology
SER
Scientific,
Engineering,

	and Research **ADM** Administrative **PUB** Public Access

Figure A-1

a. Mission Information--If the information, software applications, or computer systems in this category are altered, destroyed, or unavailable, the impact on NASA could be catastrophic. The result could be the loss of major or unique assets, a threat to human life, or prevention of NASA from preparing or training for a critical Agency mission.

b. Business and Restricted Technology Information--This category consists of information that NASA is required by law to protect. It includes information, software applications, or computer systems that support the Agency's business and technological needs. In general, if information in this category should be disclosed inappropriately, the disclosure could result in damage to employees, loss of business for NASA's partners and customers, contract award protests, or the illegal export of technology.

c. Scientific, Engineering, and Research Information--All official NASA information held by NASA employees may be released publicly only in accordance with NASA regulations; however, systems in this category do not contain information for which the release is otherwise governed by law. This category contains information that supports basic research, engineering, and technology development but is less restricted against public disclosure. Alteration, destruction, unauthorized disclosure, or unavailability of the systems, application, or information would have an adverse or severe impact on individual projects, scientists, or engineers; however, recovery would not impede the Agency in accomplishing a primary mission.

d. Administrative Information--This category includes systems, applications, and information that support NASA's daily activities, such as electronic mail, forms processing, networking, and management reporting. Administrative Information includes, but is not limited to electronic correspondence, briefing information, project/program status, infrastructure design details, pre-decisional notes, vulnerability descriptions, passwords, and internet protocol addresses. Organizations run various applications-from problem reports to configuration management tools-on administrative IT systems.

e. Public Access Information--This category contains information, software applications, or computer systems specifically intended for public use or disclosure, such as a public Web site or hands-on demonstrations. The loss, alteration, or unavailability of data in this category would have little direct impact on NASA's missions, but it might expose the Agency to embarrassment, loss of credibility, or public ridicule.

Targeting baseline requirements to the importance, value, and criticality of a system or application's information ensures that the most appropriate protective measures are applied.

A.4. Satisfying Baseline Requirements

Hardware, firmware, software, operating system capabilities, adherence to proper operations and maintenance procedures, and good user practices may satisfy requirements. The most current set of recommended tools and techniques for fulfilling these requirements can be found in the "NASA IT Security Architecture" document. (The Center IT Security Manager will have access to the most current version.)

A.5. Waiver of IT Security Requirements

System line managers may not always be able to meet the technical requirements of this manual. Older equipment, for example, sometimes does not permit management to implement all of the necessary technical and procedural features because the hardware, software, or physical controls will not accommodate them. If the cost of implementing any particular technical requirement significantly exceeds the benefits of implementation, the line manager should consider requesting a waiver.

The term "waiver," as used in the IT Security Program, does not mean that a requirement has been disregarded or set aside; rather, it means that the responsible line manager has evaluated the threats and vulnerabilities through the normal risk management process and has determined and documented the fact that the risks of not implementing a given requirement are acceptable. (See Figure A-2.) If the requirement to be waived is one described in this appendix, Center IT Security Manager concurrence will be obtained as described in paragraph A.5.3.

Risk cannot be waived, but it may be accepted.

Figure A-2

A.5.1. Waiverable Versus Non-waiverable Requirements

Some requirements for IT security cannot be waived by an authority within the NASA community. These requirements have been embodied in the Public Laws of the United States or promulgated by other directives of the Federal Government. Therefore, all organizations which process Government information, regardless of whether they are Federal or contractor entities, cannot be relieved of their responsibilities for the following:

a. Participating in an IT Security Program (Pub. L 100-235 and OMB Circular A-130).

b. Protecting personal information contained in a system of records (Pub. L 93-579, as amended).

c. Certification (or authorization) of major applications (OMB Circular A-130).

d. Assessment, analysis, and management of risks (OMB Circular A-130).

e. Personnel screening for IT access (OMB Circular A-130).

f. IT security awareness and training (Pub. L 100-235 and OMB Circular A-130).

g. Response to and reporting of IT security incidents (OMB Circular A-130).

Conversely, the requirements in this appendix are technical and physical security requirements that result from interpretation of Federal and Agency directives. A line manager may request a waiver of these provisions, if it is justified and necessary.

A.5.2. Waiver from Use of Encryption Standard

A.5.2.1. Under certain exceptional circumstances, the heads of Federal agencies may approve waivers to Federal Information Processing Standards (FIPS). (The head of such agency may redelegate such authority only to a senior official designated, pursuant to Section 3506(b) of Title 44, U.S. Code.)

A.5.2.2. Requests for waivers shall be submitted to the NASA CIO. (See paragraph 4.11, Use of Encryption Technology.)

A.5.2.3. Waivers shall be granted only when compliance with a standard would--

a. Adversely affect the accomplishment of the mission of an operator of a Federal computer system; or

b. Cause a major adverse financial impact on the operator which is not offset by Government- wide savings.

A.5.2.4. Agency heads may act upon a written waiver request containing the information detailed above. Agency heads may also act without a written waiver request when they determine that conditions for meeting the standard cannot be met. Agency heads may approve waivers only by a written decision which explains the basis on which the agency head made the required finding(s).

A.5.2.5. A copy of each such decision, with procurement sensitive or classified portions clearly identified, shall be sent to the National Institute of Standards and Technology;

ATTN: FIPS Waiver Decisions, Technology Building, Room B-154; Gaithersburg, MD 20899.

A.5.2.6. In addition, notice of each waiver granted and each delegation of authority to approve waivers shall be sent promptly to the Committee on Government Operations of the House of Representatives and the Committee on Government Affairs of the Senate and shall be published promptly in the Federal Register.

A.5.2.7. When the determination on a waiver applies to the procurement of equipment and/or services, a notice of the waiver determination must be published in the Commerce Business Daily as a part of the notice of solicitation for offers of an acquisition or, if the waiver determination is made after that notice is published, by amendment to such notice.

A.5.2.8. A copy of the waiver, any supporting documents, the document approving the waiver and any supporting and accompanying documents, with such deletions as the agency is authorized and decides to make under Section 552(b) of Title 5, U.S. Code, shall be part of the procurement documentation and retained by the agency.

A.5.3. Process for Submission of Waivers

A.5.3.1. If possible, the line manager should attempt to meet all technical requirements described in this appendix that are appropriate for the information category in question. If this is not possible, line managers should make every effort to meet these requirements by providing an equivalent degree of administrative or physical controls. If this is still not possible or the cost of controls exceeds benefits, the line manager may consider a waiver.

A.5.3.2. The waiver request should be submitted by the line manager through his or her Organization CSO, who has insight into the nature of the information at risk. If the Organization CSO accepts the justifications, then the waiver requires the Center IT Security Manager's concurrence before becoming official. Although no particular format is required, the following information is needed for proper evaluation and approval:

a. Name, location, and short description of system or application.

b. Short description of the nature of the data (sensitivity).

c. Nature of waiver requested (description of risk and control measure).

d. Time limit for which the waiver is needed.

e. Actions planned to be taken to remedy the situation that initiated the waiver request.

f. Alternatives considered to satisfy the requirement and provide an equivalent degree of protection. (Include a statement explaining why a waiver is being requested in lieu of the alternatives.)

A.5.3.3. If the IT Security Manager and the organization in question cannot resolve the disagreement, either party may appeal to the Center Director. The Center Director's decision will be final.

A.5.3.4. If a conflict that crosses Centers arises, the matter will be decided by the Manager of the PCITS. The decision of the PCITS Manager may be appealed to the Agency CIO. The Agency CIO's decision will be final.

A.6. Technical Security Requirements

A.6.1. Operating System Integrity

This section describes the requirements for ensuring operating system integrity on NASA multi-user computers.

A.6.1.1. Critical System Files Protection

Critical system files are those that are integral to the operating system, system security mechanisms, or key system services. Corrupting these files would damage the integrity of the system. Management will implement a process that accomplishes the following:

Info Category	Requirements
MSN, BRT	• Controls file access • Identifies and protects critical system files • Restricts access to critical system files to a minimum number of authorized system support personnel • Restricts access to password files to user identification (ID) management personnel • Reviews critical system file protection at least semiannually • Implements configuration control for critical system files • Maintains a list of authorized users of critical system files and verifies the list at least semiannually
SER, ADM	• Controls file access • Identifies and protects critical system files • Restricts access to critical system files to authorized users • Restricts access to password files • Reviews critical system file protection at least annually
PUB	• Ensures implementation of requirements as directed by the Center's security

	policies, procedures, and guidelines

A.6.1.2. Privileged Users and Programs

A privileged user is one who can alter or circumvent the operating system or the system's security protections. This applies to users who may have only limited privileges but who can still bypass security protections. As a result, it is vital to monitor privileged users to ensure that privileges are not abused. Privileged programs have the capability to override or bypass system security measures when executed. Management will implement a process that accomplishes the following:

Info Category	**Requirements**
MSN, BRT, SER, ADM,	• Assigns operating system privileges to a minimum number of systems personnel • Controls access to privileged programs • Maintains a list of privileged users and verifies the list at least semiannually • Ensures that system administration/support personnel do not function as system auditors
PUB	• Assigns operating system privileges to a minimum number of systems personnel • Ensures implementation of additional requirements as directed by the Center's security policies, procedures, and guidelines

A.6.1.3. Journaling and Monitoring

Most multiuser computers have the ability to record or journal important system events. These journals can be used as an audit trail to investigate system or security problems. Management will implement a process that accomplishes the following:

Info Category	**Requirements**
MSN	• Ensures system journals record security-related events • Reviews journals daily or when problems are suspected

	• Records successful and failed logons/logoffs • Records all successful and failed file opens and closes • Records all file creation/modification/deletion events • Ensures journals identify programs being executed, users, source devices, files, and the time, date, and success or failure of all access attempts
BRT	• Ensures system journals record security-related events unless specifically waived by the functional manager of the application software • Reviews journals weekly or more frequently when problems are suspected • Records successful and failed logons/logoffs • Records all successful and failed file opens and closes at the discretion of the line manager • Records critical system file modification events or attempts • Ensures journals identify programs being executed, users, source devices, files, and the time, date, and success or failure of all access attempts
SER, ADM	• Implements system journals to record security-relevant events as directed by management • Reviews journals monthly or more frequently when problems are suspected • Records successful and failed logons/logoffs • Records critical system file modification events • Ensures journals identify programs being executed, users, source devices, files, and the time, date, and success or failure of access attempts
PUB	• Ensures implementation of requirements as directed by the Center's security policies, procedures, and guidelines

A.6.1.4. System Retention/Backup

To ensure continuity of operation, copies of important software and data will be made and retained. NASA Internet server log files shall be processed according to the NASA records retention procedure. (See NPG 1441.1C, Records Retention Schedules, for retention requirements and procedures). Management will implement a process that accomplishes the following:

Info Category	Requirements
MSN	• Retains journals at least 1 year or 3 generations (whichever is longer) • Backs up the operating systems and key system services at least monthly and when modified • Retains operating system backups for at least 1 year • Stores the most recent or most recent minus one backup external to the Center
BRT	• Retains journals for at least 6 months • Backs up the operating system and key system services monthly and when modified • Retains monthly operating system backups for at least 6 months • Stores the most recent or most recent minus one backup external to the facility
SER, ADM, PUB	• Retains journals and backup system as directed by the line manager

A.6.1.5. System Shutdown/Restart

The system should provide security safeguards to cover unscheduled system shutdowns (e.g., aborts) and subsequent restarts as well as for scheduled system shutdown and operational startup. Management will implement a process that accomplishes the following:

Info Category	Requirements
MSN, BRT	• Documents system shutdown/restart procedures • Ensures only authorized personnel will shutdown/restart the system • Logs and documents all aborts and restarts
SER, ADM	• Documents system shutdown/restart procedures • Ensures only authorized personnel will restart the system
PUB	• Ensures implementation of requirements as directed by the Center's

	security policies, procedures, and guidelines

A.6.1.6. Operating System Local Modifications

Local modifications to the operating system can have security implications. If incorrectly designed or implemented, local operating system modifications may invalidate the system's security controls. Management will implement a process that accomplishes the following:

Info Category	Requirements
MSN, BRT	• Reviews and approves all operating system security modifications • Tests and/or evaluates all operating system modifications before permanent installation for impact on security • Documents all operating system security modifications
SER, ADM, PUB	• Documents all operating system security modifications as directed by the line manager

A.6.1.7. Configuration Management

Because the operating system governs the security of the system, changes to the operating system, including new releases and updates, will be controlled and monitored. To support operating system modifications, management will, as a minimum, implement a process that accomplishes the following:

Info Category	Requirements
MSN, BRT	• Documents change control for critical system files • Tests and /or evaluates and documents all operating system changes
SER, ADM, PUB	• Tests and documents all operating system changes as directed by the line manager

A.6.2. User ID Management

A user ID is a character string that uniquely identifies a user. The NASA requirements to be implemented for user ID management are listed in the following paragraphs. User ID management applies in all NASA processing environments.

A.6.2.1. User ID Approval Process/Privileges

A management control process will be implemented to ensure that all requests for user ID's are reviewed and approved by NASA line management. A list of personnel who are authorized to approve the user ID's will be furnished to the appropriate user-ID administrator. Management will implement a process that accomplishes the following:

Info Category	Requirements
MSN, BRT	• Ensures that each employee submits a formal request to the appropriate administrator for a user ID (The request will indicate the category of the user ID being requested, such as group, personal, privileged, project, application system service, or generic.) • Ensures verification of personnel screening and IT security briefing • Approves the formal request by the employee's manager (If the employee is a contractor or other non-NASA employee, the approval of the employee's NASA sponsor is also required.) • Requires all individuals assigned a user ID to sign a statement of responsibility indicating their understanding of the requirements for using and safeguarding the information to which the assigned user IDis granted access • Retains the statement of responsibility by user ID management for every active account
SER, ADM	• Requires all individuals requesting a user ID to complete the appropriate request form and sign a statement of responsibility indicating their understanding of the requirements for using and safeguarding the information to which the assigned user ID is granted access • Retains the statement of responsibility by user ID management for a minimum of 1 year
PUB	• As directed by the line manager

A.6.2.2. Group User ID's

Group user ID's are discouraged because individual accountability is lost. However, if the system is configured such that group user ID's must be used, then management will implement a process that accomplishes the following:

Info Category	Requirements
MSN, BRT	• Does not provide group user ID's without risk justification and concurrence from all functional managers of the affected data and applications • Restricts group user ID's to the minimum number necessary to conduct system operations
SER, ADM	• Restricts group user ID's to the minimum number necessary to conduct system operations
PUB	• Permits group user ID's only as directed by the Center's security policies, procedures, and guidelines

A.6.2.3. User ID Revalidation

Management will ensure that an inventory is maintained of all assigned user ID's. Management will implement a process that accomplishes the following:

Info Category	Requirements
MSN, BRT, SER, ADM	• Ensures that all user ID's are revalidated at least annually • Ensures that a statement of responsibility is on file for each person who has a user ID
PUB	• Fulfills requirements as directed by the Center's security policies, procedures, and guidelines

A.6.2.4. Disposition of Unused User ID's

Management will ensure that proper disposition is made of all unused user ID's. User ID disposition uses password lifetime (i.e., the number of days before users receive reminders to change their passwords) as the metric for user-ID-deletion decisions. The table below identifies the maximum lifetimes (in calendar days) before a user ID is removed from the system.

Info Category	**Requirements**			
	Number of days before user receives reminders to change password	Number of days that user will be reminded to change password	Number of days until user ID is suspended if user does not change password	Number of days until user ID is removed from the system
MSN	30 days	+ 30 days	60 total days	150 total days
BRT	60 days	+ 30 days	90 total days	180 total days
SER, ADM	90 day	+ 30 days	120 total days	240 total days
PUB	As determined by the line manager			

A.6.2.5. User ID Reuse

User ID's may be reassigned after removal from the system under the following conditions:

Info Category	**Requirements**
MSN	• All access rights and privileges associated with the user ID have been removed. • A 90-day waiting period has elapsed.
BRT	• All access rights and privileges associated with the user ID have been removed.
SER, ADM,	• Reassignment is in accordance with directives provided by the line manager.

PUB	manager.

A.6.2.6. Notification Upon Termination

In accordance with the following time limits, a user's supervisor will notify the manager of all systems on which the user holds a user ID when that individual is terminated, retires, or is transferred.

a. Termination for cause or reduction in force.

Info Category	Requirements
MSN, BRT	• As soon as practical but no later than the end of the day of the termination
SER, ADM, PUB	• Within 2 working days of the termination

b. Resignation/change of job/retirement -- In addition to the above requirements, line management is responsible for the disposition of user ID's assigned to employees who no longer need to access the system to perform assigned duties. Time limits for disposition of such user ID's is at line management's discretion, based on each individual case.

Info Category	Requirements
MSN	• Within 2 working days
BRT	• Within 5 working days
SER, ADM, PUB	• Within 15 working days

A.6.3. Passwords

Users are responsible for any and all activity generated through the use of their user ID's and passwords. NASA IT resources, which use passwords for user authentication, will meet the password standards defined in this section. Users
will not store passwords in program function keys or automated logon sequences.

A.6.3.1. Individual Accountability

Each individual will be held accountable for the following:

Info Category	Requirements
MSN, BRT, SER, ADM, PUB	• Providing protection against loss or disclosure of passwords in his or her possession • All activity that occurs as a result of deliberately revealing his or her user ID and password

A.6.3.2. Password Length and Composition

Management will ensure that the following password length requirements are implemented:

Info Category	Requirements
MSN, BRT, SER, ADM, PUB	• Minimum of eight characters • The eight characters will contain at least one character each from at least three of the following sets of characters: uppercase letters, lowercase letters, numbers, special characters.

A.6.3.3. Password Triviality

Management will implement a process to ensure that non-trivial passwords are used on NASA systems. A password
is considered nontrivial if it meets the following criteria:

Info Category	Requirements

MSN, BRT, SER, ADM, PUB	• The password is not equal to the user ID. • The password is not a dictionary word. • The password is not either wholly or predominantly composed of the following: - The user's ID, owner's name, birth date, Social Security Number, family member or pet names, names spelled backwards, or other personal information about the user - Any contractor name - The division or branch name - Repetitive or keyboard patterns (e.g., "abc#abc#", "1234", "qwer", "mnbvc", or "aaa#aaaa") - The name of any automobile or sports team • The password is not a word found in a dictionary of any language or a dictionary word with numbers appended or prepended to it. • The password is not the name of a vendor product or a nickname for a product.

A.6.3.4. Password Maximum Lifetime

Management will ensure that the following password lifetime requirements are implemented:

Info Category	**Requirements**
MSN	• 30 days maximum
BRT	• 90 days maximum
SER, ADM	• 1 year maximum
PUB	• 1 year maximum

A.6.3.5. Password Sharing

Management will implement a process to ensure that the following password sharing requirements are followed:

Info Category	Requirements
MSN	• Personal passwords used to authenticate identity will be owned (i.e., known) only by the individual having that identity. • Personal passwords will not be shared. • Group passwords are not allowed.
BRT	• Personal passwords used to authenticate identity will be owned (i.e., known) only by the individual having that identity. • The user ID owner may employ system features (e.g., logonby or the equivalent) to grant temporary access to another individual.
SER, ADM, PUB	• Personal passwords used to authenticate identity will be owned (i.e., known) by only the individual having that identity. • The user ID owner may employ system features (e.g., logonby or the equivalent) to grant ongoing access to another individual or may create a temporary password.

A.6.3.6. Password Reuse

Management will ensure that the following password reuse requirements are implemented:

Info Category	Requirements
MSN, BRT	• Owner must have used a minimum of 10 passwords before reuse. • 180 days must elapse before reuse.
SER, ADM, PUB	• As directed by the Center's security policies, procedures, and guidelines.

A.6.3.7. Password Storage

Management will ensure that the following password storage requirements are implemented:

Info Category	Requirements
MSN, BRT, SER, ADM	• Stored passwords will be protected in such a way that only the password system is authorized access to a password. • Passwords that are encrypted before they are stored will be protected from substitution (i.e., protection will be provided so that one encrypted password cannot be replaced with another unless the replacement is authorized).
PUB	• As directed by the Center's security policies, procedures, and guidelines.

A.6.3.8. Password Distribution

Management will implement a password distribution system that accomplishes the following:

Info Category	Requirements
MSN, BRT	• Distributes personal passwords in a way that affords reasonable protection from unauthorized disclosure • Distributes passwords in such a way that temporary storage of the password is erased, and long-term retention of the password is available only to the owner and the protected password system • Ensures that passwords are not visible at the user terminal when being typed • Distributes passwords so that an audit record, containing the user ID, date, and time of a password change, is maintained and available only to authorized personnel
SER, ADM	• Distributes personal passwords in a way that affords reasonable protection from unauthorized disclosure • Distributes passwords in such a way that temporary storage of the

	password is erased, and long-term retention of the password is available only to the owner and the protected password system • Ensures that passwords are not visible at the user terminal when being typed • Distributes passwords so that an audit record, containing the user ID, date, and time of a password change is maintained and is available only to authorized personnel
PUB	• As directed by the line manager

A.6.3.9. Password Reset

Passwords are reset when a user forgets his or her password, when evidence exists that a password has been compromised, or when management believes a password reset to be in the best interests of the security of the system. Management will implement a process that accomplishes the following:

Info Category	**Requirements**
MSN, BRT, SER, ADM, PUB	• Confirms name, location, phone number, and system user ID of the user needing reset • Provides positive identification of the user ID owner • Assigns, at the user's request, a new nontrivial password • Ensures that the password is reset by the user during first sign-on

A.6.3.10. Initial Passwords

Management will implement a process for generating and assigning the initial password for each user ID. This process will ensure the following:

Info Category	**Requirements**
MSN, BRT, SER, ADM,	• Removal of all vendor-supplied passwords • Assignment of nontrivial initial user password • Initial user password is changed during the first logon by the user

PUB	

A.6.4. Logical Access Control for MultiUser Systems

Logical access control is the process of limiting access to the resources of the system to authorized users, programs, processes, or other systems. This section applies to multiuser systems. Logical access controls also apply to networks. Network security requirements are presented in section A.7.

A.6.4.1. User Authentication

User authentication is the process by which the system verifies the user's claim of identity. The user authenticates his or her identity by presenting to the system some piece of information that is his or hers: either something known (password), something possessed (a key or token), or something he or she is (such as a biometrics measurement).

a. For **local logons** (i.e., using the user authentication to log on directly to a system), management will implement a process that accomplishes the following:

Info Category	Requirements
MSN, BRT, SER, ADM	• Requires user identification and local authentication (at least passwords) for all user ID's
PUB	• Authenticates user identification as directed by the line manager

b. For **remote logons** (i.e., accessing a second system from the first without invoking a second authentication), management will implement a process that accomplishes the following:

Info Category	Requirements
MSN, BRT, SER, ADM	• Permits, at the discretion of the remote System Administrator, remote authentication when -- - The authenticating system meets all appropriate security requirements

	of the remote system - The authenticating mechanism creates audit trails - The risk of subverting the connection between the remote and local systems is acceptable to the remote System Administrator
PUB	• Authenticates user identification as directed by the line manager

A.6.4.2. Failed Logon Attempts

Failed logon attempts are unsuccessful attempts to provide the correct logon user ID and authentication combination. Excessive failed logon attempts may indicate that an unauthorized user is attempting to access the system. Management will implement a process that accomplishes the following:

Info Category	**Requirements**
MSN	• Suspends, by system intervention, the user ID after three or fewer unsuccessful logon attempts or provides some form of system evasive action • Notifies the System Administrator of user ID suspensions • Reviews the log of unsuccessful logon attempts daily • Notifies the user ID owner of failed logon attempts
BRT	• Suspends, by system intervention, the user ID after five or fewer unsuccessful logon attempts or provides some form of system evasive action • Notifies the System Administrator of user ID suspensions • Reviews the log of unsuccessful logon attempts weekly • Notifies the user ID owner of failed logon attempts
SER, ADM	• Ensures system intervention on the user ID after five or fewer successive unsuccessful logon attempts (The line manager and IT security personnel will determine the system intervention action taken.) • Reviews the log of unsuccessful logon attempts weekly • Notifies the user ID owner of failed logon attempts

PUB	• Provides failed logon attempt requirements as directed by the Center's security policies, procedures, and guidelines

A.6.4.3. Controlled Access Protection

Controlled access protection is the ability of the system to control the circumstances under which users have access to resources. Management will ensure that all systems that are accessed by more than one user will provide the following controlled access protection when those users do not have the same authorization to use all of the information on the system:

Info Category	**Requirements**
MSN, BRT, SER, ADM	• Provides individual electronic accountability through identification and authentication of each system user • Provides audit trails or a journal of security-relevant events • Provides the ability to control a user's access to information
PUB	• Provides controls as directed by the Center's security policies, procedures, and guidelines

A.6.4.4. Default File Protection

Default file protection is the access control the system places on a file when the data owner does not take explicit action. Management will implement a process that accomplishes the following:

Info Category	**Requirements**
MSN, BRT	• Sets system default file protection parameters to grant write access to the file owner and to necessary operating system components • Sets system default file protection parameters to prevent read and execute access by anyone except the file owner and necessary operating system components

SER, ADM	- Sets system default file protection parameters to grant write and execute access to the file owner and to necessary operating system components
PUB	- Implements requirements as directed by the Center's security policies, procedures, and guidelines

A.6.5. Information Management and Protection for Multi-User Computers

A.6.5.1. An application processes data, giving it form, structure, and meaning. The application derives its information category from the data it processes or contains. The computer system derives its information category level from the applications it handles or stores. All data or information has an owner and in some cases an application owner. Owners are responsible for making decisions concerning protection and sharing. Owners may either apply the protections themselves or designate other appropriate personnel, such as data custodians or System Administrators, to implement protections.

A.6.5.2. Software tools are a special type of application. Various software tools used to develop and support a specific application (such as flight design computation routines) are owned by that application owner. Tools that are shared by all system users (such as a language compiler) are owned by the group with the primary responsibility for the host system.

A.6.5.3. The paragraphs that follow define the requirements and responsibilities of the data owner and the application owner.

A.6.5.4. Data Owner Requirements/Responsibilities

The data owner will do the following:

Info Category	**Requirements**
MSN, BRT	- Specify the information category of the application/information (subject to review by the Center IT Security Manager) - Specify the security protections to be implemented - Identify authorized users and custodians - Identify and protect private data from unauthorized disclosure - Ensure that hard copy output (including electronic media) is controlled as necessary - Ensure that implementation of file access controls as appropriate

SER, ADM	• Specify the information category of the application/information (subject to review by the Center IT Security Manager) • Specify the security protections to be implemented • Identify authorized users and custodians, as appropriate • Protect private data from unauthorized disclosure
PUB	• Ensure that implementation of requirements as directed by the Center's security policies, procedures, and guidelines

A.6.5.5. Application Data Backup/Recovery

Application data backup/recovery defines the owner's requirements to restore the application/information after a system (hardware/software) malfunction or compromise of integrity. In support of this activity, the application owner will ensure the following:

Info Category	**Requirements**
MSN	• Retain at least 3 generations of operating system releases or 1 year (whichever is longer) of backups • Store the most recent backup or most recent minus one in a facility external to the Center • Define frequency of application data backups • Define and test data recovery procedures
BRT	• Retain at least three generations of backups • Store the most recent backup or most recent minus one in an external facility • Define frequency of application data backups • Define and test data recovery procedures
SER, ADM, PUB	• Ensure that implementation of requirements as directed by the Center's security policies, procedures, and guidelines

A.6.6. Commercial Off-the-Shelf (COTS) Software

COTS software is software that has been developed, tested, placed on the market, and advertised as a saleable product. Before installation, COTS software will be tested on the system according to the requirements in paragraph A.6.6.1. Maintenance of COTS software will be done according to the requirements in paragraph A.6.6.2.

A.6.6.1. Software Acceptance Testing

Software acceptance testing for IT security features provides a measure of assurance that the software product correctly provides the advertised capabilities. Management will implement a process to ensure the following:

Info Category	Requirements
MSN, BRT	• A test or inspection of available source code is performed to ensure that the program and installation scripts are free from malicious or unauthorized code. • Function, reliability, and penetration tests are included in a test plan and performed. • Testing and verification of security controls and application features are witnessed by appropriate personnel and documented.
SER, ADM	• Tests are performed that show the program is free from malicious or unauthorized code (e.g., scanning for known viruses, backdoors, logic bombs, and Trojan code).
PUB	• Tests, as directed by the Center's security policies, procedures, and guidelines, are conducted.

A.6.6.2. Maintenance of COTS Software

Software maintenance (i.e., modifications and updates) increases the risk that errors, accidents, and intentional acts can occur. To keep these risks at a minimum, management will implement a process that accomplishes the following:

Info Category	Requirements
MSN, BRT	• Reviews, evaluates, installs, and tests all vendor-recommended application updates in accordance with paragraph A.6.6.1 • Ensures that the software is controlled by a configuration management

	process
SER, ADM, PUB	• Implements requirements as directed by the Center's security policies, procedures, and guidelines

A.6.7. Public Domain Software

Public domain software includes software acquired from the Government or non-government sources, often at no charge, when the source takes no responsibility for the integrity or maintenance of the software. Public domain software is often written by enthusiasts and distributed by users' groups, or via electronic mail, local bulletin boards, Usenet, or other electronic media. Public domain software is a common carrier of malicious code. NASA line managers will establish a process for approving the use of public domain software. The process should at least verify the source of the software as trusted, check for viruses, and test the software to ensure it works properly.

A.6.7.1. User Workstations

Management will implement a process that accomplishes the following:

Info Category	Requirements
MSN, BRT	• All public domain workstation software will be approved by an officially appointed staff member who will ensure that the software is free of malicious code before installation. • All solicited or unsolicited sample programs will be approved by an officially appointed staff member who will ensure that the software is free of malicious code before installation.
SER, ADM, PUB	• All workstation software not acquired through the normal Center procurement processes will be approved before installation in accordance with requirements established by the staff element in question.

A.6.7.2. Mainframes

Management will implement a process that accomplishes the following:

Info Category	Requirements
MSN, BRT	- All public domain mainframe software will be approved by an officially appointed staff member who will ensure that the software is free of malicious code before installation. - All solicited or unsolicited sample programs will be approved by an officially appointed staff member who will ensure that the software is free of malicious code before installation.
SER, ADM, PUB	- All mainframe public domain software not acquired through normal Center procurement processes will be approved before installation in accordance with requirements established by the staff element in question.

A.6.8. Customer/Contractor-Supplied Software

Customer/contractor-supplied software is software that is developed or customized by either in-house or contractor-supplied services, including universities.

A.6.8.1. Formalized Project Life-Cycle Development

Each line manager engaged in formal life-cycle project development will ensure that basic security requirements are integrated throughout the software's life cycle. Management will implement a process that accomplishes the following:

Info Category	Requirements
MSN, BRT, SER, ADM	- Establishes security requirements for applications - Reviews decisions on implementation of security controls during definition, design, programming, and testing - Reviews and enforces operational security controls
PUB	- Reviews and enforces operational security controls

A.6.9. Encryption of Unclassified Data

Encryption needs to be used on sensitive/critical data only if the risk analysis process for that system so dictates. When encryption is employed, the algorithm specified in FIPS 46-1, currently the Data Encryption Standard (DES), will be used for production systems.

A.6.9.1. Requirement

If encryption is employed, the responsible line manager will implement a process that accomplishes the following:

Info Category	Requirements
MSN, BRT, SER, ADM	• Ensures that a key management process is established and maintained • Ensures that a data recovery process is maintained to ensure that NASA information is accessible
PUB	• Encryption of data at this level is not normally applicable

A.6.9.2. Key Management

Key management refers to the generation, distribution, storage, and destruction of keys used to encrypt and decrypt data. Management will implement a process that accomplishes the following:

Info Category	Requirements
MSN, BRT, SER, ADM	• Affords electronically stored cryptographic keys the same level of security • Designates and records a key owner for each cryptographic key • Ensures that the key owner distributes the cryptographic key to authorized personnel only • Delivers the cryptographic key to its recipients in a manner that is at least as secure as logon password distribution
PUB	• Encryption of data at this level is not normally applicable

A.6.9.3. Password Encryption

Management will implement a process that accomplishes the following:

Info Category	Requirements
MSN, BRT, SER, ADM	• Encrypts passwords if it is possible for either privileged or nonprivileged users to browse memory or disk storage where passwords are kept • Encrypts password files on backup tapes if it is possible for either privileged or nonprivileged users to browse the tapes
PUB	• Encrypts passwords if directed by the Center's security policies, procedures, and guidelines • Encrypts passwords if the system on which they are used is connected to a system of higher sensitivity

A.6.9.4. Private Data

Private data are data that has disclosure restrictions such as Privacy Act, source selection, contractor proprietary, or medical data. Management will implement a process that accomplishes the following:

Info Category	Requirements
MSN, BRT, SER, ADM	• Encrypts private data if the system has no other mechanism for providing controlled browse access protection to the data • Encrypts private files on backup tapes if the tape library system has no other mechanism for providing controlled browse access protection to the data Note: "Browse access protection" may be provided by appropriate physical security measures for systems without external interfaces.
PUB	• Encryption of data at this level is not normally applicable.

A.6.10. Centralized Operations for MultiUser Systems, Servers, and Mainframes

Centralized operations refer to the operational tasks and ancillary functions that support multi-user systems, servers, and mainframes (also known as host systems). Operational tasks include, but are not limited to, the setup, operations (e.g., start, stop, configure, bypass/recover), and monitoring of console control units and peripherals. Operational tasks may be accomplished from a centralized location or a remote console. Ancillary tasks include, but are not limited to, job and event scheduling and processing, job quality control, magnetic tape cleaning and certification, magnetic disk module inspection and cleaning, tape library operation, and the coordination of media retention and accountability tasks. The requirements that follow are to be fulfilled by the managers of multiuser systems.

A.6.10.1. Documentation

The line manager will implement a process that accomplishes the following:

Info Category	**Requirements**
MSN, BRT	• Retains complete operating system and appropriate application documentation • Develops, uses, and maintains operating procedures and checklists • Maintains a complete inventory of system software and application software • Maintains and reviews a list of system security software problems as directed by management • Reviews applications annually for changes in information categories • Develops and maintains risk analysis, risk reduction, and contingency plans • Maintains a list of personnel responsible for system and application software
SER, ADM	• Retains complete operating system documentation • Develops and maintains operating procedures and checklists • Maintains a complete list of systems' applications • Maintains and reviews a list of system security software problems as directed by management • Reviews applications annually for changes in information categories • Develops and maintains risk analysis, risk reduction, and contingency plans • Maintains a list of personnel responsible for system and application software

PUB	• Reviews applications annually for changes in information categories • Maintains a list of personnel responsible for system and application software • Maintains documentation as required by the Center's security policies, procedures, and guidelines

A.6.10.2. Privileged Operations

The line manager will implement a process that accomplishes the following:

Info Category	Requirements
MSN, BRT, SER, ADM	• Controls access to operator consoles • Ensures that operators do not transfer privileged activity outside the operations area without proper authorization • Ensures that only the operations group is authorized to disable console logging and that the event is logged when performed • Documents and reports IT security incidents to the Organization Computer Security Official, management, and Center IT Security Manager • Maintains and archives (both manual and automatic) console logs • Reviews operator console logs regularly
PUB	• Controls access to operator consoles • Ensures that operators do not transfer privileged activity outside the operations area without proper authorization • Ensures that only the operations group is authorized to disable console logging and that the event is logged when performed • Documents and reports IT security incidents to the Organization Computer Security Official, management, and Center IT Security Manager

A.6.10.3. Console Logon

The line manager will implement a process that accomplishes the following:

Info	Requirements

Category	
MSN, BRT, SER, ADM	• Ensures that operators do not transfer privileged activity outside the operations area without proper authorization • Ensures that only the operations group is authorized to disable console logging and that the event is logged when performed • Documents and reports IT security incidents to the Organization Computer Security Official, management, and Center IT Security Manager • Maintains and archives (both manual and automatic) console logs • Reviews operator console logs regularly
PUB	• Ensures that only the operations group is authorized to disable console logging and that the event is logged when performed • Documents and reports IT security incidents to the Organization Computer Security Official, management, and Center IT Security Manager • Reviews operator console logs regularly

A.6.10.4. Media Storage

Media may be stored in a variety of environments, including libraries, offices, laboratories, and computer rooms.
Whenever it is stored, the media must be protected from destruction, damage, theft, unauthorized modification,
and unauthorized access.

Operations management will implement a process that accomplishes the following:

Info Category	Requirements
MSN, BRT	• Ensures that the media library is in an environmentally controlled area • Ensures that only authorized personnel have access to the media • Provides an inventory accounting system for all media entering or leaving a media storage facility when appropriate • Maintains and verifies a media inventory at least semiannually • Identifies all media with an external label and, when applicable, an internal label • Provides a visual means of identification (i.e., labels) for all media containing private data

	• Ensures that media containing restricted access data are degaussed (erased)/overwritten before being returned to use or excessed • Protects media from theft, vandalism, and natural disasters
SER, ADM	• Ensures that the media are in an environmentally controlled area • Ensures that only authorized personnel access the media • Ensures that media containing restricted access data are degaussed (erased)/overwritten before being returned to use or excessed • Protects media from theft, vandalism, and natural disasters
PUB	• Protects media from theft, vandalism, and natural disasters

A.6.10.5. Job Input

Protection, control, and integrity of data by operations personnel during an input preparation process are very important. Therefore, whenever operations personnel are required to set up and process job input to support a customer or user, operations management will implement a process that accomplishes the following:

Info Category	**Requirements**
MSN, BRT, SER, ADM	• Ensures that input comes from an authorized source
PUB	• Ensures the implementation of requirements as directed by the Center's security policies, procedures, and guidelines

A.6.10.6. Job Output

Controlling the output of processed information helps ensure the continued protection of the information after it leaves
the processing area. To support this function, operations management will implement a process that accomplishes the following:

Info Category	Requirements
MSN	• Attaches the appropriate cover sheet to all output containing restricted access data • Distributes the output only to authorized personnel • Destroys all output for which there are restrictions on disclosure and which has not been distributed after a time period specified by line management • Produces only the minimum number of copies requested to support the distribution
BRT, SER, ADM	• Attaches the appropriate cover sheet to all output containing private data • Distributes restricted access output to only authorized personnel • Destroys any restricted access data that has not been distributed after a time period specified by line management
PUB	• Ensures the implementation of requirements as directed by the Center's security policies, procedures, and guidelines

A.6.11. Workstation Security Requirements

Workstations include, but are not limited to, systems used to support desktop processing (personal computers), LAN's, and servers typically used in an office or laboratory environment.

A.6.11.1. Single-User Workstations

A single-user workstation is one that may be used by only one person at a time, though many people may have access. Where single-user workstations are installed, management will do the following:

Info Category	Requirements
MSN, BRT, SER, ADM	• Implement a risk management program commensurate with the information category being processed • Establish backup and recovery requirements • Ensure that virus detection software is installed on all applicable

	workstations
PUB	- Ensure that system configuration is documented - Establish backup requirements - Ensure that virus detection software is installed on all applicable workstations

A.6.11.2. Multiuser Workstations

A multiuser workstation, also known as a host system, is one that can be accessed simultaneously by other workstations. Where multiuser workstations are installed, management will implement a process that accomplishes the following:

Info Category	**Requirements**
MSN, BRT	- Documents system configuration - Ensures that virus detection software is installed in the workstation where applicable - Ensures that backup requirements are established - Implements a risk management program appropriate for the category being processed - Assigns a System Administrator - Identifies each user by a unique user ID and password - Provides secure backup storage external to the processing area - Ensures that critical data backups are placed in secure storage
SER, ADM	- Documents system configuration - Ensures that virus detection software is installed in the workstation where applicable - Ensures that backup requirements are established - Develops a contingency plan
PUB	- Documents system configuration - Ensures that virus detection software is installed in the workstation where applicable - Establishes backup requirements

A.6.12. Authorization to Process (or Certification/Recertification)

Each IT system that processes information by or on behalf of the Federal Government must have written authorization and periodic re-authorization to process by the appropriate line management official. (This is also known as certification and recertification to process.)

A.6.12.1. The authorization and periodic re-authorization should take the form of a letter to the Center IT Security Manager summarizing the results of the risk analysis; any residual risk; planned, budgeted, and scheduled corrective actions; and a certification statement of risk acceptance to process. For small systems, a cover letter or an approval sheet with the signatures of the responsible line manager and any affected "data owners" attached to the IT Security Plan can be used.

A.6.12.2. The authorization and periodic re-authorization are required in writing upon attaining initial operational capability and at least every 3 years (or upon significant change) thereafter before the system is permitted to process or continue to process information.

A.6.12.3. Copies of the authorization and re-authorization will be filed with the Center IT Security Manager.

A.7. Network Security Requirements

This section presents the network security guidelines and baseline requirements that apply to NASA networks. Network IT resources sometimes perform multiple functions, such as a server that also does routing and protocol conversion. In these cases, the most restrictive requirements will apply. These requirements supplement, rather than take precedence over, the requirements of any individual systems connected to the network (sometimes referred to as network nodes or hosts).

A.7.1. Network Security Elements

The security of a network or any attached node consists of three elements: integrity (e.g., ensuring that transmitted data is received intact), availability (e.g., network services are performed within an acceptable timeframe), and confidentiality (e.g., preserving the privacy of information). NASA's networks will be designed to provide integrity and availability. Confidentiality, if needed, will be provided by the owner of the node system or application.

A.7.1.1. Network Data Integrity

Data integrity is preserved when information transmitted over the network is protected during transmission from unauthorized modification, whether by accident, error, or willful alteration. NASA networks will provide integrity through the use of established protocols and network devices with proven error detection capabilities. Systems or applications with more rigorous needs may employ additional integrity safeguards, such as message authentication codes or digital signatures, at the option of the node system or application owner.

A.7.1.2. Network Availability

Network availability depends on protection against loss of or damage to network components and network abuse. NASA's networks are protected from damage to, or loss of, network components by physically protecting components and providing redundant connections. Protective measures against network abuse include user authentication and network monitoring. Availability and integrity are security concerns as well as operational concerns. The loss of availability and integrity due to equipment failure or improper maintenance is beyond the scope of this document.

A.7.1.3. Network Confidentiality

Types of information that require privacy protection are passwords, which could be captured and used to gain unauthorized access to NASA computers; personnel records, which are protected by the Privacy Act; financial data, such as payroll information; sensitive electronic mail, such as performance evaluations; proprietary, contract, or other data dealing with procurements, such as source selection information; and other data with restrictions on its distribution, such as export controlled information. When private data must be transmitted over networks, protective measures will be employed based on the results of the system's risk assessment. The implementation of cost-effective controls is the responsibility of line management.

A.7.2. Establishing a Network Security Architecture

All NASA networks will use a network architecture that addresses network security concerns. The network security guidelines provided in this NPG are the basis for network node security requirements. "Node" refers to an individually addressable computer that is capable of supporting one or more user sessions. Management should do the following when establishing any NASA network architecture:

a. Implement safeguards to protect information resources, including the network's equipment, against misuse or attack to a level commensurate with their importance.

b. Identify the goals and priorities for network operations such as--

1) protecting Government resources.

2) maintaining operational support requirements and network connectivity at an acceptable level of risk.

3) supporting legal or administrative enforcement efforts.

c. Assign a LAN Manager who is responsible for network operations, network security issues, and network connection policies.

d. Establish an isolated network for public read-only access to selected computers.

e. Maintain accounting information for monitoring, detecting attempted attacks, and allowing

backtracking to the source of attacks.

f. Support incident response and administrative or legal enforcement efforts.

g. Establish controls to ensure that only authorized individuals have access to NASA network support resources.

h. Assess security implications before allowing connections to the networks or changing network configurations.

i. Document the importance, value, and criticality of systems by subnets or segments. Since some networks or network segments may have higher security requirements than others, each node will comply with all of the security for the network or network segments to which it connects. Additionally, network connections for nodes supporting MSN and BRT information category applications and data will be isolated from other network nodes' security perimeter (such as a firewall) to ensure that the proper level of network isolation is provided.

j. Establish an approval process for users, vendors, and contractor organizations wishing to connect to a Center's networks. Also, establish a process for handling deviations, such as deviations from the network security baseline requirements, that will require approval by Center LAN managers and concurrence from the Center IT Security Manager.

k. Develop, implement, and test a Network Emergency Response Plan that will ensure a timely response to network emergencies.

l. Provide an "outer layer" of security (e.g., a firewall) for Center nodes; however, ensure that line managers of nodes understand that they retain ultimate responsibility for their system's security.

A.7.3. Network Security Baseline Requirements

To protect all of its information resources, Centers will establish and maintain a network architecture that includes security for both network components and connected systems. This architecture is commonly referred to as a "firewall architecture"; however, the total architecture is usually made up of many components, such as Virtual Private Networks (VPN), an isolation LAN or Demilitarized Zone (DMZ), and a boundary system. Management and appointed staff will do the following:

a. Establish a security perimeter between Center networks and networks external to the Center.

b. Establish acceptance of externally initiated interactive and file transfer sessions across security perimeters (through approved connection points, otherwise known as boundary systems).

c. Track connections when they cross the security perimeter.

d. Restrict services allowed to cross the perimeter (e.g., services that are not specifically allowed will be denied.)

e. Support public-access read-only information servers, or special boundary systems, and test them to ensure that they do not pose an unacceptable threat to the computers inside the security perimeter.

f. Support protected message routing for all Center networks, ensuring that messages on protected networks are not accessible to unauthorized users outside of the security perimeter. (This will not be the sole means of protection for the networks within the security perimeter.)

g. Establish an approval process for supporting organizations wishing to connect to a Center's networks inside the security perimeter. The Center's LAN line manager must have established guidance for connectivity which addresses other external connections that may exist, such as dial-in modems and any deviations from the established network architecture.

h. Test networks or network segments within the security perimeter to ensure that they comply with established network security requirements. This does not require all nodes on a network to have the same information category. Networks or network segments within the security perimeter may have higher security requirements.

i. Review external connections to the Center. Networked nodes operating within a Center's security perimeter cannot have dial-in services that bypass any of the security guidelines described above. This includes both dial-in modem and facsimile (FAX) service into computer systems. Standalone FAX machines that do not connect to a computer or computer network are exceptions to this rule.

j. Identify networked nodes with stricter controls in order to provide them with notification of problems such as specific attacks or scheduled outages.

k. Establish restrictions and controls to prevent networked nodes from having "back door" connections to untrusted systems. Network nodes cannot be simultaneously connected to a protected network and a nonprotected network. Physical disconnection from all nonprotected networks is required prior to the establishment of a connection to a node on a protected network.

A.7.4. Network Multiuser System, Server, and Mainframe Requirements

Network multiuser systems, servers, and mainframes have some additional security requirements imposed on them solely by operating as a node on a network. This section details the network-related security requirements for nodes by the information category of the system. These requirements are in addition to system requirements found earlier in this appendix. Total network security for systems handling MSN, BRT, SER, and ADM categories of information will be ensured through the protection mechanisms on the systems themselves and the additional protection provided through the network boundary system(s).

A.7.4.1. Authentication Requirements

Authentication is the process by which a computer verifies the identity of a user. The process generally consists of the computer prompting the user for a user ID and, at minimum, a password. Management will implement a process that accomplishes the following:

Info Category	Requirements
MSN, BRT, SER, ADM	• Ensures that network devices detect and close broken sessions • Prohibits unattended dial-in diagnostics that bypass normal authentication • Accepts dial-in connections and connections from public networks (such as the Internet) only via a boundary system • Optionally, may accept user authentication from the boundary system without requiring additional authentication
PUB	• Ensures that network devices detect and close broken sessions • Disables dial-in diagnostics that bypass normal authentication when they are not in use, or as directed by line management • Employs password management features as specified in paragraph A.6.3

A.7.4.2. File Transfer and Remote Logon Protection Requirements

Services provided by the network include such processes as file transfer and remote logon. These services require special protection. Management will implement a process that accomplishes the following:

Info Category	Requirements
MSN, BRT, SER, SDM	• Prohibits inbound or outbound file transfer from unauthenticated users (i.e., no anonymous file transfer) • Restricts access to any privileged network software to a list of specifically authorized users • Allows only specifically authorized users to import software • Employs digital signatures or multiple checksums to ensure the integrity of file transfer • Restricts "proxy" or "trusted" logons • Prohibits inbound remote command execution without user authentication
PUB	• Allows inbound or outbound file transfer from unauthenticated users only to a restricted set of directories • Restricts access to any privileged network software to authorized users • Restricts "proxy" or "trusted" logons as specified in paragraph A.7.4.1 • Restricts inbound remote command execution without user authentication

A.7.4.3. Connection Requirements

Network attachment increases the number of threats to which a system may be vulnerable. Therefore, certain security precautions must be taken before a system is attached to a network. Management will implement a process that accomplishes the following:

Info Category	Requirements
MSN, BRT, SER, ADM	• Ensures that the risks associated with connecting to the proposed network/node are acceptable • Ensures that "trusted" network partners (e.g., those the local system trusts to authenticate users) have implemented security protections equivalent to or acceptable to the local system
PUB	• Evaluates network connections according to IT security policies, procedures, and guidance

A.7.4.4. Additional Requirements for Boundary Systems

Boundary systems are critical elements in providing a security perimeter for networks. The boundary system provides isolation and security services to the systems within the security perimeter. As such, the boundary system's own internal configuration integrity must be maintained. Boundary systems must meet the mission information category (MSN) protection requirements listed previously in paragraphs A.7.4.1 through A.7.4.3 as well as the following additional requirements:

a. A boundary system will use extended user authentication to authenticate incoming user sessions destined for nodes inside the security perimeter.

b. Individual user accounts will not be supported on the boundary system. Only administrator accounts and service accounts will be supported.

c. File transfer (ftp) and terminal emulation (telnet) sessions may be supported in both directions through the boundary system.

d. Outbound user sessions may be supported with no extra authentication required.

e. Electronic mail between users on opposite sides of the boundary (security perimeter) may be supported but only through a store-and-forward service on the boundary system.

A.7.5. Network Component Security Requirements

A network consists of many devices, called components, connected together with various types of media, such as coaxial or twisted-pair cable. All of these components support the network; however, some of them also perform security functions. Certain components enhance network security by limiting the flow of network traffic for security reasons. They include devices that perform user authentication and devices that provide security monitoring. These critical components are worthy of protection themselves, not because the data they transmit is of a certain information category.

A.8. Physical Security Requirements

Physical security provides protection of IT resources from human, natural, and accidental damage. The primary intent of this section is to present guidelines and examples of the things individuals and managers must consider when analyzing potential hazards in computer facilities, laboratories, and office environments that use IT resources. It is not the intent of this appendix to specify requirements for facility construction. Construction requirements are adequately covered in separate documentation. More information should be obtained from the CCS. Some facility items, however, are traditionally included in IT security audits and inspections. These items are covered in this section and include entry control, protection of resources from fire and water damage, housekeeping, and storage and protection of resources. This section presents prudent and reliable physical security guidelines that are compatible with good risk management practices. The areas that management must address for the physical security of IT resources are those that pertain to entry control, protection of IT resources from fire and water, electric power, facility housekeeping, and computer resource protection.

A.8.1. Entry Control

Entry control is the process by which only authorized individuals are allowed physical access to IT resources. Procedures must recognize the difference among environments, such as computer rooms, offices, laboratories, and mechanical/electrical equipment rooms. Regardless of the environment, line management is responsible for the data, applications, hardware, and other equipment of which the facility is comprised. The following paragraphs discuss appropriate controls for the different types of environments.

A.8.1.1. Controlled Access Areas

Controlled access areas usually house high-value equipment or equipment that performs mission- or life-critical functions. Only personnel with defined business needs should be authorized to enter a controlled access area. Authorized personnel will be issued appropriate badges and/or personal recognition methods to permit entrance. A list of people granted ongoing access should be maintained and reconciled at least annually. Personnel who need to enter only occasionally should be escorted or issued temporary badges. A record should be kept of their visits.

A.8.1.2 Laboratory Areas/Computer Rooms

For the purpose of this document, a laboratory/computer room is defined as a common area where a collection of IT resources is housed and an access mechanism is not required. A facility manager is designated, but a single point of responsibility for each terminal or workstation is not generally assigned. Several users may share the resources. In this environment, the laboratory manager is responsible for implementing appropriate controls and procedures for the entire laboratory.

A.8.1.3 Office Areas

Each computer resource in an office area will be assigned to an individual user who is responsible for those resources. This individual is responsible for protecting the equipment and information processed by the equipment. Information may be protected in a variety of ways: locking the workstation (if the workstation keys are unique); employing software access controls on the workstation; locking the office housing the workstation; or keeping the information on removable media which are locked in a desk, file cabinet, or safe as necessary when unattended.

A.8.2 Protection of IT Resources from Fire and Water

Proper fire barriers within, above, and below the operational area plus adequate fire alarm, overhead fire sprinklers, and fire suppression systems should be in place. Properly positioned, hand-operated extinguishers should be available. Water may accumulate under the raised floor; therefore, adequate drains or alarms should be provided. Waterproof covers should be provided for all appropriate IT resources located in the facility, and adequate floor panel lifters should be available. Appropriate smoke alarms should also be installed as well as under-floor water detectors.

A.8.3 Electric Power

A.8.3.1 The operation of facility equipment depends on the availability of adequate and reliable electric power. The criticality of the data processing functions performed by a facility will determine the degree of power reliability required. Because the loss of electrical power may result in an immediate cessation of equipment operations, a thorough analysis of potential points of utility failure and available backup measures (i.e., installation of an uninterruptible power supply) should be conducted. Special attention should be given to emergency shutdown controls within a facility. In case of a power failure, emergency (i.e., battery-powered) lights should be installed and procedures in place to periodically check their operation.

A.8.3.2 In major facilities, a prominently labeled master control switch(es) should be located at each principal exit from the electronic equipment area. These switches should disconnect power to all electronic equipment and are in addition to any emergency shutdown for individual machines or other units of equipment. Switches should be provided at egress points from the electronic equipment area to permit the shutdown of air handling equipment. Manually activated exhaust and ventilating systems should have startup and shutdown switches at the egress points.

A.8.4 Facility Housekeeping

Facility housekeeping plays an important part in implementing a sound physical security program. Food or beverages should not be allowed in facilities. Combustible supplies of cleaners, paper boxes, and cards should be in equipment areas only as needed. Approved storage areas should be provided external to the facility for storing large numbers of combustible items in accordance with safety regulations.

A.8.5 IT Resource Protection

A.8.5.1 IT resources include storage media as well as hardware and software. Magnetic media and their data should be protected against fire, erasure, or inadvertent/malicious damage by humans.

A.8.5.2 All media of value should be handled with care and stored in protected areas with adequate accounting procedures and environmental controls applied. Media containing backups should be stored in a separate facility. Facilities located in different buildings may store each other's software backups.

APPENDIX B. Acronyms and Abbreviations

ADM	Administrative
BRT	Business and Restricted Technology
CCS	Center Chief of Security
CIO	Chief Information Officer
COMSEC	Communication Security
COTR	Contracting Officer`s Technical Representative
COTS	Commercial Off-the-Shelf
CSO	Computer Security Official
DAA	Designated Approval Authority
DES	Data Encryption Standard
DMZ	Demilitarized Zone
EO	Executive Order
FIPS	Federal Information Processing Standards
IRM	Information Resource Management
IT	Information Technology
ITS	Information Technology Security
ITSM	Information Technology Security Manager
IPSO	Information Processing Service Organizations
LAN	Local Area Network
MSN	Mission
NISPOMSUP	National Industrial Security Program Operating Manual Supplement
NIST	National Institute of Standards and Technology
NPD	NASA Policy Directive
NPG	NASA Procedures and Guidelines
NRP	NASA Resource Protection

NSA	National Security Agency
NTISSP	National Telecommunications and Information Systems Security Publications
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PCA	Program Commitment Agreement
PCITS	Principal Center for Information Technology Security
PUB	Public Access
RFP	Request for Proposal
RAM	Random Access Memory
ROM	Read Only Memory
SER	Scientific, Engineering, and Research
SOP	Security Operations Plan
SOW	Statement of Work
VPN	Virtual Private Network
WAN	Wide Area Network

APPENDIX C. Glossary

ACCEPTABLE RISK -- A level at which there is reasonable assurance of management acceptance. Acceptability of risk is a judgment call, based on a risk assessment and local details (e.g., security specifications, system testing results, appropriateness, and compliance with applicable policies).

ACCESS -- The ability to obtain or change information or data. Within a system, "access" is the interaction between a subject (e.g., person, process, or device) and an object (e.g., record, file, program, or devise) that results in the flow of information from one to the other. The nature or type of access can be read, write, execute, append, modify, delete, and create.

ACCOUNT REQUEST DOCUMENT -- A formal request in writing or via electronic mail requesting access to a system or major application.

ACCREDITATION -- The written authorization from a DAA to activate or operate a computer processing National Security Information (i.e., classified information): (i) in a particular security mode, (ii) with a prescribed set of technical and nontechnical security safeguards, (iii) against a defined threat, (iv) in a given operational environment, (v) under a stated operational concept, (vi) with stated connections to other automatic information systems/networks, and (vii) at an acceptable level of risk for which the accrediting official has formally assumed responsibility. The accreditation statement affixes security responsibility with the accrediting official and indicates that due care has been taken for security.

ADMINISTRATIVE INFORMATION -- A category of knowledge used to determine the baseline requirements for IT security. It applies to systems, applications, and information that support NASA's daily business activities. Examples include electronic mail and management reporting.

APPLICATION -- A set of computer commands, instructions, and procedures used to cause a computer to process a specific set of information. Application software does not include operating systems, generic utilities, or similar software that are normally referred to as "system software."

APPLICATION OWNER -- The highest level manager whose responsibility is the functional operation of an application. By definition, every "major application" has an owner.

AT RISK - The probability that harm or loss to a system is reasonably likely.

AUDIT TRAIL -- A record of computer activities. Normally, audit trails are chronological. They should be sufficient to enable the reconstruction and examination of a sequence of events, environments, activities, procedures, or operations from inception to final result.

AUTHENTICATION -- (1) The validation and confirmation of an IT user's claim of identity, occasionally referred to as personal authentication. (2) The validation and identification of a computer network node, transmission, or message.

AUTHORIZATION -- The privilege granted to a subject (e.g., individual, program or process) by a designed official to do something, such as access information based on the individual's need to know.

AUTHORIZATION TO PROCESS -- A written statement from a line manager which indicates that a system or "major application" can become operational. The statement is based on an acceptable level of risk.

AVAILABILITY -- The state wherein information, data, and systems are in the place needed by the user, at the proper time, and in the form that the user requests.

BASELINE REQUIREMENTS -- Sets of technical, procedural, and physical IT security measures intended to ensure a reasonable level of security for a system. These requirements are derived from "best practices" used by industry and the Government.

BOUNDARY -- A designated perimeter that is used to differentiate between internal and external entities. In IT security planning, a boundary is a border that is used to identify the IT resources for which an IT security official is responsible. It identifies the scope of an IT security planning effort.

BOUNDARY SYSTEM -- One that is topographically located at the crossroads between an internal LAN/WAN and the Internet. A boundary system is usually associated with routing, firewalling, and other security-oriented purposes. It provides isolation and security services to the systems within a security perimeter.

BUSINESS AND RESTRICTED TECHNOLOGY INFORMATION -- A category of knowledge used to determine the baseline requirements for IT security. It applies to systems, applications, and information that support the Agency's business and technological needs, such as payroll and personnel.

CERTIFICATION -- A written acknowledgment (by a NASA management official) that there is reasonable assurance that an automated application and its automated environment (i) meet all applicable NASA and other Federal policies, regulations, and standards covering security; and (ii) have been tested and technically evaluated thoroughly enough to demonstrate that the installed security controls are adequate.

CLASSIFIED INFORMATION -- Data or information that requires safeguarding in the interest of national security. This information is TOP SECRET, SECRET, or CONFIDENTIAL, in accordance with EO 12958. In this document, "classified information" refers specifically to information for which NASA is the classification authority.

COMMERCIAL OFF-THE-SHELF (COTS) SOFTWARE - That which a vendor has developed, tested, placed on the market, and advertised as a salable product. These software packages are readily available to consumers. They are developed with the typical customer(s) in mind and are usually not geared towards specific company concerns or issues.

COMPONENTS -- Pieces of hardware and/or software that when integrated together make up an entire system.

COMPUTER CRIME -- The use of system(s), software, or network(s) to deliberately commit criminal activities, which may include, but are not limited to, the compromise of system privileges (e.g., root access), compromise of information protected by law (e.g., International Traffic in Arms Regulations, Privacy Act Data, procurement sensitive data), denial of service of major IT resources, child pornography, and malicious destruction of NASA data and/or information.

COMPUTER SECURITY ACT (Public Law 100-235) -- This was enacted by Congress to provide for a computer standards program within the National Bureau of Standards, to provide for Governmentwide computer security and to provide for the training in security matters of persons who are involved in the management, operation, and use of Federal computer systems, and for other purposes.

COMSEC -- Measures and controls taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications. NOTE: Communications Security includes cryptosecurity, transmission security, emission security, and physical security of related material.

CONFIDENTIALITY -- Holding sensitive data in confidence such that distribution is limited to those individuals or organizations with an established need to know.

CONFIGURATION CONTROL -- The management process of controlling the specific elements that compose IT and controlling changes to these elements; the process that ensures that only authorized and approved changes of or to these elements are made. Configuration control includes, but is not limited to, hardware, firmware, and software elements.

CONTINGENCY PLAN -- See "Information Technology Security Contingency Plan."

CONTROLLED ACCESS PROTECTION -- The ability of a system to control the circumstances under which users have access to computer resources.

CONTROLS -- Protective measures used to improve security by reducing risks, also known as "safeguards," "countermeasures," or "security features."

CRITICAL SYSTEM FILES - Those that are necessary in order for a system to perform regular tasks, including boot-ups, network logon(s), and all other normal standard operations.

CRYPTOGRAPHY -- The principles, means, and methods for rendering information unintelligible and for restoring encrypted information to intelligible form.

DAEMON -- A Unix process that runs in the background in support of other processes that users may invoke using different commands. Daemons are usually active as long as the system is active. Typically, they do "housekeeping" on a computer.

DATA OWNER -- The individual (organizational line manager) responsible for the confidentiality, integrity, and availability of a specific set of data. This individual is responsible for making judgments and decisions on behalf of the organization with regard to the data's information category level, criticality, use, protection, and sharing. Typically, this individual is a member of the organization directly supported by the data. Often this individual maintains the data and ensures its accuracy. All data have a data owner.

DEGAUSSING -- Reducing the magnetic flux density to zero by applying a reverse magnetizing field. Degaussing erases all data from data storage media so that it is no longer retrievable from the media.

DENIAL OF SERVICE -- A type of malicious attack that causes the interruption and/or stoppage of regular ongoing IT system activities.

DESIGNATED APPROVAL AUTHORITY (DAA) -- Person(s) that is charged with accrediting information resources for processing National Security Information(i.e., classified information).

DISPOSAL OF IT ASSETS -- Releasing the accountability (excessing, turned in for repair, or transferring to another organization) of IT equipment and ensuring the elimination of any controlled information and software stored on this equipment.

ENCRYPTION -- Any procedure used in cryptography to convert plain text into cipher text in order to prevent anyone other than the intended recipient from reading that data.

END USER - A person who relies on computer systems to conduct duties or business activities. They represent the typical user within the system architecture.

EXPORT CONTROL -- Restrictions pertaining to the export of U.S. goods and technical data, including, but not limited to, encryption software, computer hardware, software applications, and technology-oriented products.

EXTERNAL CUSTOMERS - Those who are not affiliated in any way with the entity with which they are conducting business. In this document, these customers may include Federal, State, or local governments; international partners; other NASA organizations; or organizations in the private sector.

FACILITY -- Designated locations in which a logical group of one or more IT resources are located.

FEDERAL INFORMATION PROCESSING STANDARDS (FIPS) -- Issued by the NIST after approval by the Secretary of Commerce regarding management and operations of IT resources. (Also called FIPS PUBS.)

FEDERAL INFORMATION PROCESSING STANDARDS (FIPS) 140 -- General Security Requirements for Equipment Using the Data Encryption Standard specifies the security requirements that are to be satisfied by a cryptographic module used within security systems to protect unclassified information.

FEDERAL MANAGERS' FINANCIAL INTEGRITY ACT (Pub.L. 97-255) -- Etablishes specific requirements with regard to management controls which should be an integral part of the entire cycle of planning, budgeting, management, accounting, and auditing. Controls are to be established that reasonably ensure that (i) obligations and costs comply with applicable law, (ii) assets are safeguarded against waste, loss, unauthorized use or misappropriation, and (iii) revenues and expenditures are properly recorded and accounted for. The Act encompasses program, operational, and administrative areas as well as accounting and financial management. The controls should support the effectiveness and the integrity of every step of the process and provide continual feedback to management.

FIREWALL -- A computer, router, and/or other communications device that filters access to a protected network. They may also consist of a collaboration of such components geared toward protecting networks from unwarranted intrusion from the Internet while allowing users inside the network access to services on the Internet, such as Web and e-mail services.

FIRMWARE -- Programming instructions that are stored in a ROM unit rather than being implemented through software. Firmware is not specific to any one computer component; it is a part of the ROM of almost all computer components.

FREEWARE -- Computer software packages that are distributed by their respective vendors/developers. Freeware packages are normally distributed via the World Wide Web and the Internet with no implied costs to the entity downloading the package.

GENERAL SUPPORT SYSTEM -- A set of information resources under the same management control that share common functionality and require the same level of security controls.

GROUP USER ID -- A system identification that is shared among a group of individuals for logging on to a computer, application, or set of files. Establishing one requires a justification and concurrence from the system's line manager.

GOVERNMENT INFORMATION -- Knowledge or facts created, collected, processed, disseminated, or disposed of both by and for the Federal Government.

HOSTILE PROBES -- The act of using one or more systems to scan targeted systems or networks with intent to conduct or to gather information for unauthorized activities. They are often targeted against networks (LAN's) rather than single stand-alone systems. They may return information that may provide information on system vulnerabilities.

"IMAGE" BACKUPS -- A dump of the entire contents of a system's disk media. For example, in Unix a command is used to make an image (exact copy) of the "system" disk. The disks must be physically identical for this to work. The command "dd" copies the specified input file to the specified output with possible conversions.

IMPORTED SOFTWARE -- That which is not developed by NASA that enters the NASA community.

INDIVIDUAL ACCOUNTABILITY -- The condition that enables activities on an IT system to be traced to those who can then be held accountable for their actions.

INFORMATION -- Any communication or reception of knowledge, such as facts, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in any medium, such as computerized databases, paper microfilm, tapes, disk, memory chips, RAM, ROM, microfiche, communication lines, and display terminals.

INFORMATION CATEGORY -- A designation for the type, sensitivity, and criticality of information processed by a system or "major application." In this document, information categories are as follows: Mission; Business and Restricted Technology, Scientific, Engineering, and Research, Administrative, and Public Access.

INFORMATION COMPROMISE -- That which occurs when information has been made available to person(s) and/or systems(s) who are not the intended audience. Compromises usually occur when a system has been successfully hacked into (i.e., security controls have been compromised).

INFORMATION PROCESSING SERVICE ORGANIZATION (IPSO) -- Groups that provide computer-related services, such as business systems, electronic mail, electronic forms, applications servers, telecommunications, local and wide area networks, data storage, scientific computing resources, and desktop services.

INFORMATION RESOURCE MANAGEMENT -- The planning, budgeting, organizing, directing, training, and control of information and related resources, such as personnel, equipment, funds, and technology.

INFORMATION TECHNOLOGY -- Hardware and software operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information on behalf of the Federal government to accomplish a Federal function, regardless of the technology involved, whether by computers, telecommunications systems, automatic data processing equipment, or other.

INFORMATION TECHNOLOGY (IT) RESOURCES -- Data and information; computers, ancillary equipment, software, firmware, and similar products; facilities that house such resources; services, including support services; and related resources used for the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data. This includes telecommunication systems, network systems, and human resources. (Also called Automated Information Resources.)

INFORMATION TECHNOLOGY (IT) SECURITY CONTINGENCY PLAN -- For emergency response, backup operations, and postdisaster recovery, it is created, maintained, and tested as part of the IT security planning process to ensure the availability of critical resources and facilities necessary for the continuity of processing in an emergency situation. The document, developed in conjunction with application owners and maintained at the primary and backup system facility, describes procedures and identifies the personnel necessary to respond to abnormal situations (including disasters). Contingency plans assist managers to ensure that data owners continue to process (with or without computers) mission-critical applications in the event that computer support is interrupted.

INFORMATION TECHNOLOGY (IT) SECURITY INCIDENT -- An adverse event or situation associated with a system which poses a threat to the integrity, availability, or confidentiality of data or systems and that results in a failure of security controls; an attempted, suspected, or actual compromise of information; or the waste, fraud, abuse, loss, or damage of Government property or information.

INFORMATION TECHNOLOGY (IT) SECURITY PLAN -- A detailed document that specifies the security goals and implementation of security controls for a given IT system. It describes a system's risks, the controls in place to counter risks, any risks that have not been addressed, and justification for not addressing risks. This is the end product of the IT security planning process. A line manager or data owner is responsible for developing and maintaining this document.

INTERNATIONAL PARTNER -- Foreign entities with which business and/or research is conducted. Foreign partners may include individuals, small firms, large corporations, and/or foreign governments.

INTEGRITY -- The state that exists when computerized data is the same as that in source documents or has been correctly computed from source data and has not been exposed to accidental or malicious alteration or destruction.

KEY MANAGEMENT -- The generation, distribution, storage, and destruction of keys used to encrypt and decrypt data. (See "Encryption.")

LIMITED PRIVILEGE ACCESS -- That which is granted to a user to use system-level commands and files to bypass security controls for part of a system.

LOCAL LOGON -- The identification and authentication sequence that authorizes a user's access to a computer but requires that the sequence be performed at the designated local computer. This cannot be done by way of an intermediary computer.

LOGIC BOMBS -- A resident computer program that triggers the perpetuation of an unauthorized act when particular states of the system are realized.

LOGON -- The identification and authentication sequence that authorizes a user's access to a computer. Conversely, "logoff" is the sequence that terminates user access to the system.

LOGONBY -- A feature provided by a Virtual Machine (VM) security package that allows an authorized person to use the password of his or her own personal account to log on to another account. This feature eliminates the need to share passwords for an account that will be used by several people.

MAJOR APPLICATION -- That which requires special attention to security due to the risk and magnitude of the harm that would result from the loss, misuse, or unauthorized access to or modification of the information in the application.

MAJOR INFORMATION SYSTEM -- That which requires special management attention because of its importance to an Agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of Agency programs, finances, property, or other resources. This designation is assigned by the Agency or Center CIO for OMB A-11 reporting.

MALICIOUS CODE -- Computer program instructions created with the intent of malice or unauthorized acts towards the targeted system(s) and may be written in many computer languages, including but not limited to, C, C++, Visual Basic, Assembly Language, and Java.

MEDIA -- Any and all materials in which data and/or information may be stored and may include floppy disks, CD-ROMS, hard drives, software manuals, and papers.

MISSION CRITICAL SYSTEM -- Computer systems/networks that are vital for the planning and/or implementation of a mission. Systems of this nature are highly critical, require "special management attention," and should be secured, using the best possible security measures.

MISSION INFORMATION -- A category of knowledge used to determine the baseline requirements for IT security. It applies to systems, applications, and data that support the planning and implementation of a mission, such as human space flight and launch operations.

MISUSE -- The use of computer systems and or facilities that do not comply with Center or Agency guidelines, standards, and/or policies.

NATIONAL INDUSTRIAL SECURITY PROGRAM OPERATING MANUAL SUPPLEMENT (NISPOMSUP) -- This document provides special security measures to ensure the integrity of National Security Information and imposes controls supplemental to security measures prescribed in the NISPOM for classified contracts. In this document, NASA has selected the NISPOMSUP guidance as the baseline for security measures to protect National Security Information processed by IT resources(i.e., classified processing).

NASA RESOURCE PROTECTION (NRP) PROGRAM -- Provides reasonable, affordable, practical, and responsible protection, within acceptable risk, to those vital

NASA resources, that cannot reasonably be replaced, or that have unique capabilities to support NASA goals. (Reference NPG 1620, Security Procedure and Guideline.)

NATIONAL SECURITY INFORMATION - Reference Executive Order 12958.

NODE -- A general point on a network that occupies one or more Internet Protocol addresses, such as computers, servers, routers, and printers.

NONPRIVILEGED ACCESS -- Restricted access granted by a system for users to conduct business. Non-privileged access allows users to use and access the most common commands and files while restricting access to system-level commands and files. This access does not allow users to bypass security controls.

OFFICIAL BUSINESS USE -- The use of Government property, such as computers and facilities, for conducting business in accordance with official policies and procedures of the respective Government agency.

OMB A-130 -- OMB Circular Number A-130 which provides uniform Governmentwide information resources management policies as required by the Paperwork Reduction Act of 1980, as amended by the Paperwork Reduction Act of 1995, 44 U.S.C. Chapter 35.

OMB A-130, APPENDIX III -- Establishes a minimum set of controls to be included in Federal automated information security programs, assigns Federal agency responsibilities for the security of automated information; and links agency automated information security programs and agency management control systems established in accordance with OMB Circular No. A-123.

ORGANIZATION COMPUTER SECURITY OFFICIAL -- The designated Government person who is assigned the task of managing and maintaining the security of IT resources within a component.

PASSWORD -- A protected word, phrase, or a string of symbols that is used to authenticate the identity of a user. When associated with a particular user ID, it is considered proof of authentication to use the capabilities associated with that user ID.

PENETRATION TEST -- A planned attempt by authorized officials to circumvent security controls in order to identify security weaknesses that need to be corrected.

PHYSICAL CONTROLS -- Barriers and deterrents used against threats to IT resources and sensitive information which include, but are not limited to, locks, guards, badges, and alarms.

PRIVACY ACT OF 1974 (Pub. L. 93-579) -- A law enacted by Congress to protect against an invasion of privacy through the misuse of records by Federal agencies which allows a citizen to learn how records are collected, maintained, used, and disseminated by the Federal Government. It also permits an individual to gain access to most personal information maintained by Federal agencies and to seek amendment of any incorrect or incomplete information.

PRIVATE DATA -- That which is intended only for selected person(s) to access and is usually protected by setting permissions either on individual file(s) and/or entire directories within systems connected to a network.

PRIVILEGED ACCESS -- That which is granted to a user so that files, processes, and system commands are readable, writable, executable, and/or transferable. This allows a user to bypass security controls.

PRIVILEGED ACTIVITY -- Any capability and/or process that is executed with given privileged access controls.

PROCEDURAL CONTROLS -- Security measures that IT system managers impose through personnel actions rather than by electronic means. Also called administrative controls. Examples of procedural controls include using sign-in logs, documenting configuration changes, and filling out checklists.

PROPER USE -- The use of Government property in accordance with the policies, procedures, and guidance specified by the respective Government agency.

PROXY LOGONS -- An identification and authorization sequence that takes the place of another and has the authority to act in place of the other.

PROXY SERVER -- A network computer which provides resources and is authorized to act in place of another while delegating and substituting functional duties as an agent of the original.

PUBLIC ACCESS INFORMATION -- A category of knowledge used to determine the baseline requirements for IT security. It applies to data and information that are freely available to the general public to access. Systems that handle Public Access information still require security controls.

PUBLIC DOMAIN SOFTWARE -- Packages unprotected by copyright or patent that have little or no restrictions and are free for downloading and use. These packages are often written by enthusiasts and distributed by users' groups, or via electronic mail, local bulletin boards, Usenet, or other electronic media.

PUBLIC TRUST POSITIONS -- Those that have the potential for action or inaction that could affect the integrity, efficiency, or effectiveness of Government activities, iIncluding those positions that require special computer access privileges. Candidates for these positions must be screened for suitability.

RE-AUTHORIZATION -- A repeated authorization procedure that a line manager must do periodically to continue operation of a system or "major application system." (See "Authorization to process.")

REMOTE LOGON -- Accessing one system by way of another without having to log on to the destination host. For example, accessing System B by logging on to System A and linking directly from System A to System B without logging on a second time.

RESTRICTED ACCESS DATA -- Information whose distribution is restricted by regulation, policy, or laws.

RISK -- The probability that a system is vulnerable to a threat that may cause harm or loss. If there is no vulnerability, regardless of the seriousness of the threat, there is no risk. Conversely, if there is no threat, regardless of the seriousness of the vulnerability, there is no risk.

RISK ANALYSIS -- The breakdown and dissection of perceived risks with regard to IT security issues which involves identifying system's vulnerabilities and potential system compromises and indexing the findings in a detailed report.

RISK ASSESSMENT -- The determination of security risk exposure done as part of IT security planning. This determination usually requires a list of automated information resources and a list of potential security impacts on those resources from adverse events to determine the anticipated level of harm or loss that, in turn, is used by management to determine whether the IT security risk is acceptable. Methodologies used in this determination may be qualitative, quantitative, or a combination of both. Often called security "risk analysis."

RISK REDUCTION -- The lessening of security exposure to an acceptable level. This requires the identification, analysis, selection, approval, and implementation of cost-effective IT security protective measures. Sometimes called "safeguard implementation."

RISK REDUCTION ANALYSIS -- A process done during IT security planning that evaluates the risks identified during a risk assessment and results in recommendations on methods for elimination or reduction.

RISK SUMMARY -- A condensation of findings resulting from a risk assessment. A risk summary provides specific information about the individual and overall risk(s) of a system.

SCIENTIFIC, ENGINEERING, AND RESEARCH INFORMATION -- An information category used to determine the baseline requirements for IT security. It applies to systems, applications, and information related to data collected by scientists, engineers, and researchers. Although all official NASA information held by NASA employees may be released publicly only in accordance with NASA regulations, this category is not otherwise governed by law. Information of this type is primarily research data and is used to advance further research.

SECURITY CONTROLS/SECURITY MEASURES -- Steps taken in order to ensure an acceptable level of security for systems and networks. Some examples might be to install network-monitoring software, shadow password files, restrict non-local access, and install anti-virus software.

SECURITY INVESTIGATION - The means or procedures used to determine the suitability of an individual to have privileged or limited privilege access and to hold a "Public Trust" position. Conducted by the Center Chief of Security.

SECURITY PERIMETER -- A designated border that is used to identify the IT resources that an IT Security Plan covers. It identifies the scope of an IT security planning effort.

SENSITIVE UNCLASSIFIED -- Information, data, or systems that require protection due to the risk and magnitude of the harm or loss that could result from unauthorized disclosure, alteration, loss or destruction but has not been designated as classified for national security purposes.

SENSITIVITY -- The degree of importance, criticality, or confidentiality assigned to a given piece of data or information.

SHARED RISKS -- The vulnerabilities and potential security breakdowns that are common to a group of users and/or systems.

SHAREWARE -- Computer software programs that are freely distributed either on the Internet, by mail, or by any other means, are unique in that they contain only some parts of the retail software package, and are often used as a method of advertisement.

SIGNIFICANT CHANGE -- A modification, deletion, or addition to a system which may result in reducing the effectiveness of protective controls or in making additional protective controls necessary. Examples of significant changes include, but are not limited to, relocation to other facilities, major modification of the existing facilities, introduction of new equipment, addition or deletion of external interfaces, changes to system network connectivity, installation of new operating system software, patches to applications, new releases of software, installation of new application software, introduction of more sensitive data, or a substantial change to the system's risk posture that might affect others on the same network.

SPECIAL MANAGEMENT ATTENTION -- Exceptional oversight that is required by some systems due to the risk and magnitude of harm that would result from the loss, misuse, unauthorized access to or modification of the data in a system.

SYSTEM -- In this document, this term is used to mean an interconnected set of information resources under the same management control which shares common functionality and requires the same level of security controls. Normally includes hardware, software, information, data, applications, telecommunication systems, network communications systems, and people.

SYSTEM COMPROMISE -- A situation in which a system has been accessed by an individual who is not authorized to conduct such activities. Usually the result of some exploited vulnerability of the system.

SYSTEM LOGS -- Records that contain information about various activities including, but not limited to, logon information, root-privileged processes, and network connection(s) information. They are usually kept in order to investigate system functionality issues and intrusion or probe attempts. Also referred to as "journals" or "audit logs."

SYSTEM PRIVILEGES -- Unlimited access to a system by yielding all commands and permissions of files. Someone with system privileges can modify the computer's operating system, system audit logs, system configurations, account privileges, account passwords, data files, software, or applications; add or delete accounts; install or delete software and applications; or alter the system's security controls outside those abilities normally authorized for an individual's account. (System privileges are equivalent to root privileges on Unix Operating Systems.)

TECHNICAL CONTROLS -- Security measures provided by the manufacturer of a system or software application to protect the systems data or information. These are inherent in the operating system or purchased software applications (e.g., the ability to restrict account access or the ability to force password changes at predetermined intervals).

THREATS -- An indication of impending danger or harm. Within the context of IT security, they may be viewed as perceived potential dangers and are events or circumstances, whether internal or external, that have the potential to cause harm to a system or to its associated applications or information.

TRAP DOOR -- Pieces of code written into applications or operating systems to grant programmers access to programs without having to go through the normal methods of access authentication. They are used primarily by programmers for debugging or monitoring code that is in development and are also referred to as "back doors."

TROJAN CODE -- Programming code developed to perform a task while using functions and/or displays to make it seem as if it is running other tasks. The program appears to be doing what the user wants, but it is doing something else entirely.

TROJAN HORSE -- A computer program with an apparently (or actually) useful function that contains additional (hidden) functions that surreptitiously exploit the legitimate authorizations of the invoking process.

TRUSTED LOGONS -- Procedures that are conducted after preauthentication requirements have been verified and accepts the user as authorized to log on to the system.

UNAUTHENTICATED USERS -- Those whose identity has not been verified to the system or process. and must be treated as foreign entities and be subjected to all security precautions.

UNAUTHORIZED ACCESS -- The accessing of system(s) and/or processes using methods that are not approved or certified by the system and/or System Administrators.

USER ACCOUNT -- Authority granted to an individual to access a system or software application. Typically granted by system administrators with the approval of the system's line manager. To access an account, a user needs to be authenticated, usually by providing a password.

USER AUTHENTICATION -- A process by which a system receives validation of a user's identity.

USER IDENTIFICATION (USER ID) -- A unique character string used in a computer to identify a user which is not normally protected as private/privileged information, but is normally unique within the system.

VIRUS -- Self-propagating software that parasitically attaches itself to authorized software and has three functional components: mission, trigger, and self-propagation. It is capable of doing anything that software can do, both good and bad, once it is activated in a system.

VITAL RECORDS -- Those that are designated with a highest level of importance and may contain proprietary organizational information, personal employee information, and/or trade secrets. They may also provide information needed to get a system back into operation in the event of a disaster.

VULNERABILITY -- A weakness in a system or software application that could be exploited to compromise security processes or controls that protect the system and the information it handles.

WAIVER -- The determination and documentation by the responsible line manager that the risks of not implementing a given requirement present an acceptable risk to the system in question and to other systems to which it may be networked. Accomplished by evaluating the threats and vulnerabilities through the normal risk management process.

This index uses paragraph numbers instead of page numbers.